

# Cơn ác mộng 4.0: Kỷ nguyên công nghiệp hoá

# 「RANSOMWARE」

— Bất kỳ ai cũng có thể trở thành kẻ tấn công

01

# Tấn công RaaS leo thang mạnh mẽ

<sup>1</sup>RaaS: Ransomware as a Service

Ransomware **không còn là một cuộc tấn công đơn lẻ.**

Ngày nay, Ransomware được lặp đi lặp lại theo cùng một kịch bản:

1



Đánh cắp dữ liệu

2



Yêu cầu tiền chuộc

3



Rò rỉ dữ liệu

4



Nâng mức yêu cầu

RaaS là **tâm điểm** của làn sóng tấn công đang thay đổi.



02

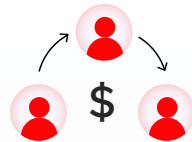
# Cách «RaaS» hoạt động thực tế

Quy trình tấn công được thiết kế  
và phân vai một cách tinh vi.



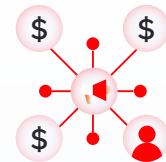
## Nhà cung cấp

Phát triển ransomware và duy trì hạ tầng tấn công



## Người môi giới

Mua đi bán lại quyền truy cập và thông tin đăng nhập



## Kẻ thực thi

Mua dịch vụ và triển khai chiến dịch tống tiền

▶ Kỹ thuật không còn là rào cản, tấn công dễ dàng hơn.



03

# Làn sóng 「RANSOMWARE」 lan rộng toàn cầu

## ▶ Châu Âu – Nhiều sân bay lớn tê liệt vì ransomware

- Hàng loạt chuyến bay bị hoãn hoặc hủy tại Brussels, Heathrow và nhiều sân bay khác

## ▶ Nhật Bản – Tập đoàn Asahi bị tấn công ransomware

- Hệ thống sản xuất và phân phối bị gián đoạn
- 27 GB dữ liệu bị đánh cắp

## ▶ Hàn Quốc – Ngân hàng bị tấn công ransomware

- Dịch vụ bị ngưng trong 4 ngày
- 24 trên 79 yêu cầu bồi thường đã được giải quyết, ước tính thiệt hại 9.000 USD



04

## Chiến lược phòng thủ nhiều lớp

- 1 Đào tạo và nâng cao nhận thức cho nhân viên**  
Thực hiện mô phỏng tấn công tăng khả năng phản ứng sự cố
- 2 Tăng cường hệ thống sao lưu**  
Đảm bảo dữ liệu luôn được sao lưu, sẵn sàng phục hồi
- 3 Ngăn chặn lây lan trong hệ thống nội bộ**  
Khoanh vùng tác động, kiểm soát truy cập ở mức tối thiểu
- 4 Ngăn chặn sớm các hướng tấn công tiềm ẩn**  
Giám sát lỗ hổng và vá lỗi trước khi bị khai thác



05

# EG-Platform từ VNETWORK

Giải pháp email duy nhất đáp ứng 100% bộ tiêu chuẩn bảo mật của ITU và được các tổ chức uy tín trên thế giới khuyến nghị sử dụng



Giám sát & phát hiện mối đe dọa theo thời gian thực



AI/Machine Learning phân tích hành vi người dùng



Mô hình bảo mật Zero-trust

(phát hiện URL, file, QR độc hại, v.v.)



Nền tảng bảo mật đồng bộ, khép kín và toàn diện

## Email Gateway Platform

Giải pháp bảo mật Email chiều gửi và nhận, ứng dụng AI/Machine Learning

Bảo mật Email ngay →

### Summary of Diagnosis

[Company Name]'s email security solution detected [n] suspicious emails from [dd-mm-yyyy] to [dd-mm-yyyy] of total [n] total emails. [n] caution dangerous emails were detected. Such emails potentially harm your computer or network through personal data breaches. Therefore, we advise you to update your email security solution, or if you are not sure, we strongly encourage you to implement a solution that can block such emails.

### Overall Results of Email Diagnosis

Cautionary Email	First-level Filter
Dangerous Email	Business/Promotional Spam
	Malware (Malicious)
	Malicious URL (Ransomware)
	Conditional Block
Tampered Email	Forged Header
	Sender Location Change
	Look-alike Domain

### Inbound Emails by Vulnerability

Information Leakage [n]

### Top 5 Users Requiring Caution

[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	Please check the email security solution to ensure that both business and promotional emails are blocked. If there are any emails that have not been blocked, it is recommended to update the email security solution.
	Malware	To proactively block dangerous emails classified as malicious activities, it is recommended to utilize an email security solution with the capability to analyze all behaviors of email.
	Malicious URL	To proactively block malicious URLs, it is recommended to set up an option to receive emails only from authenticated senders when dealing with a significant volume of emails containing links.
	Ransomware	By allowing only emails that meet specific criteria, such as a fixed IP or other specified conditions, you can proactively block emails classified as ransomware.
Tampered Email	Forged Header	We recommend implementing an email security policy that prioritizes blocking emails where the actual sender's email address differs from the one visible to the recipient.
	Sender Location Change	We recommend offering a separate notification feature for email originating from high-risk countries to provide users with an alert and take necessary precautions as a default response.
	Look-alike Domain	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 patterns.