VNETWORK Playbook

EGPlatform
Email Gateway Platform

Cơn ác mộng 4.0:

Kỷ nguyên công nghiệp hoá

「RANSOMWARE」

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

vnetwork.vn

01

Tấn công 「RaaS」[1] leo thang mạnh mẽ

[1]RaaS: Ransomeware 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.

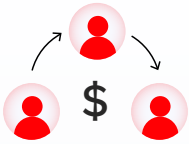
02

Cách 「RaaS」 hoạt động thực tế

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

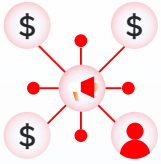
Nhà cung cấp

Phát triển ransomware và duy trì hạ tầng tấn công



Người môi giới

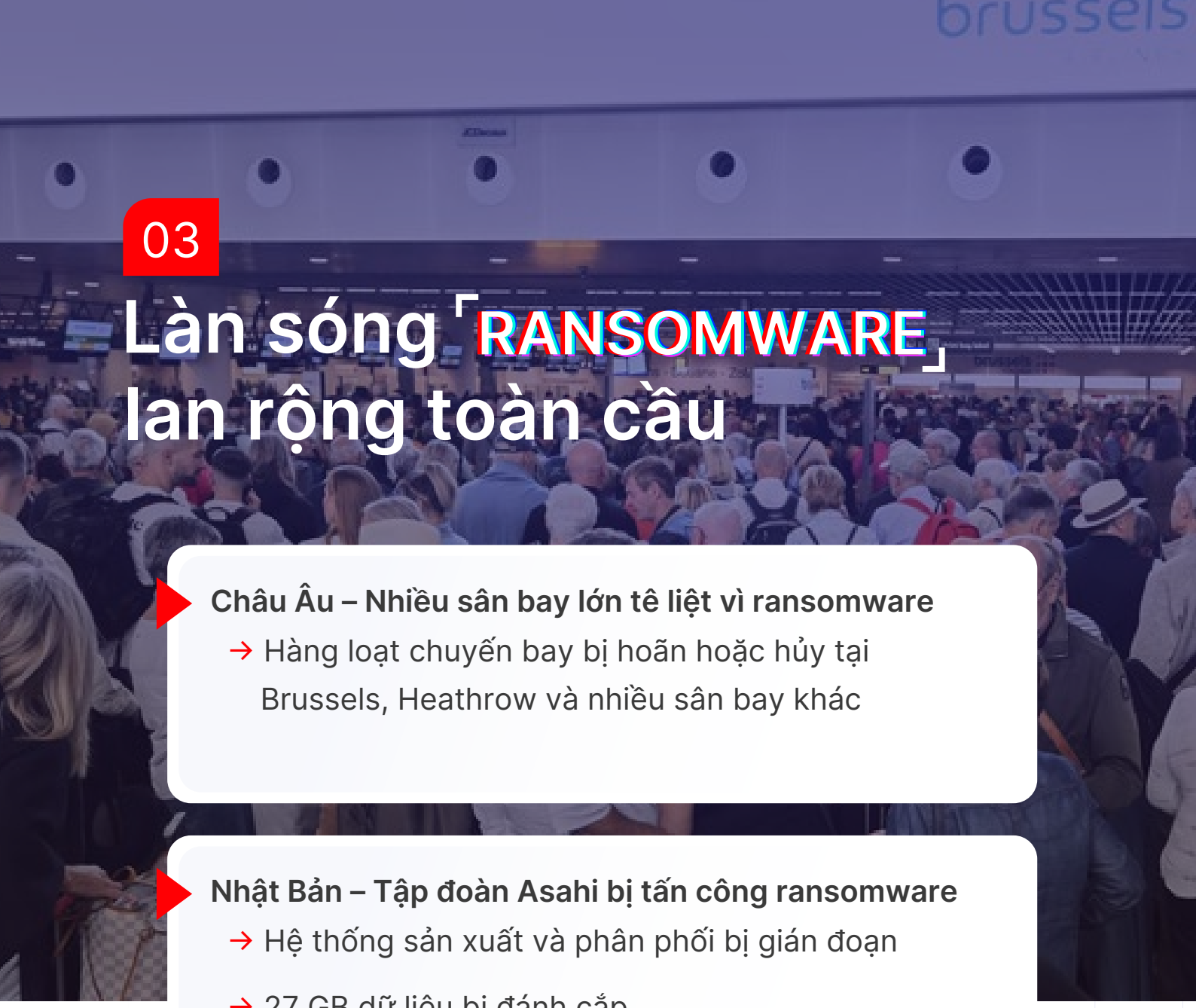
Mua đi bán lại quyền truy cập và thông tin đăng nhập



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 →