viettel security

WHITE PAPER

RANSOMWARE GUIDELINE:

GIẢI MÃ CÁC VẤN ĐỀ XUNG QUANH RANSOMWARE & CHIẾN LƯỢC ỨNG PHÓ TỪ NGẮN HẠN ĐẾN DÀI HẠN

Tài liệu cung cấp những kiến thức và kinh nghiệm thực tiễn từ góc nhìn của các chuyên gia giàu kinh nghiệm xử lý sự cố Ransomware, giúp doanh nghiệp nắm bắt nhanh chóng những sai lầm hay gặp phải khi ứng phó với Ransomware, từ đó lên chiến lược, kịch bản phòng chống hiệu quả từ ngắn hạn tới dài hạn!

viettelcybersecurity.com

viettel security

MỤC LỤC

viettel security

Ransomware GUIDELINE

Trong 6 tháng đầu năm 2024, hệ thống **Viettel Threat Intelligence** ghi nhận nhiều chiến dịch tấn công Ransomware mã hóa dữ liệu vào hạ tầng ảo hóa của tổ chức, doanh nghiệp - đặc biệt chỉ trong quý 1 đã **tăng 70% so với cùng kỳ năm 2023** với nhiều phương thức tấn công đa dạng, khiến nhiều doanh nghiệp, tổ chức không kịp trở tay.

Ransomware có thể chỉ bắt đầu bởi hành vi đơn giản như một cái nhấp chuột vào email lừa đảo nhưng hoàn toàn có thể làm lung lay một thương hiệu.

Vậy làm thế nào để doanh nghiệp có thể chủ động phòng tránh và hạn chế tác động của Ransomware? Tất cả có trong Ransomware Guideline - Những kiến thức cơ bản nhưng thiết yếu mà mọi doanh nghiệp cần có để tự bảo vệ mình khỏi các cuộc tấn công mã độc Ransomware ngày càng tinh vi và khó lường.

Tuyên bố miễn trừ trách nhiệm

Hướng dẫn này hoàn toàn phục vụ mục đích duy nhất là chia sẻ thông tin kỹ thuật cho cộng đồng an toàn thông tin (ATTT) và các tổ chức doanh nghiệp nhằm nâng cao nhận thức về ATTT cũng như có các phương án đảm bảo đề phòng cho các vấn đề về rủi ro ATTT mạng. Mọi cáo buộc khác nội dung của báo cáo này đều không đúng với mục đích xuất bản của chúng tôi. Báo cáo có sử dụng một số thông tin thu thập được trong quá trình cung cấp dịch vụ cho khách hàng của công ty An ninh mạng Viettel (Viettel Cyber Security - VCS)

I. Tổng quan

1. Ransomware là gì? Lịch sử hình thành và các giai đoạn phát triển của Ransomware

Ransomware là một loại **phần mềm độc hại (malware)** mà tội phạm mạng sử dụng để mã hóa dữ liệu của nạn nhân, khiến họ không thể truy cập vào các tệp tin của mình. Sau đó, kẻ tấn công sẽ yêu cầu nạn nhân trả một khoản tiền chuộc (thường là bằng tiền điện tử) để có được khóa giải mã dữ liệu.

Tấn công mã hóa dữ liệu hay Ransomware đã xuất hiện từ rất lâu. Theo chuyên gia của VCS, **quá trình phát triển của Ransomware có thể chia ra làm 3 giai đoạn chính:**

- **Từ năm 2016 trở về trước:** Các tổ chức tấn công nhỏ lẻ, hình thức phát tán và xâm nhập đơn giản, với phương thức cài cắm mã độc làm khóa màn hình, pop-up thông điệp đòi tiền chuộc hoặc mã hoá dữ liệu trên các máy tính đơn lẻ.
- **Từ năm 2017:** Đánh dấu sự bùng nổ của Ransomware. Lợi dụng lỗ hổng nghiêm trọng trong giao thức SMB của hệ điều hành Windows, mã độc Ransomware có tên WannaCry cùng các dòng mã độc biến thể tương tự đã phát triển nhanh chóng trên phạm vi toàn cầu, lây nhiễm cho hàng trăm ngàn máy tính trên hàng trăm quốc gia.
- **Trong khoảng 3 năm trở lại đây:** Ransomware kết hợp với APT, sử dụng các kỹ thuật tiên tiến để xâm nhập vào tổ chức, khai thác các lỗ hổng, thậm chí lỗ hổng 0-day, và nằm lại trong hệ thống trong thời gian dài. Tin tặc cắm rễ, biết mọi ngóc ngách, của cải của doanh nghiệp đặt ở đâu, đồng thời, được hậu thuẫn rất lớn về tài chính để hoạt động.

Đặc điểm nổi bật của các nhóm tấn công Ransomware hiện nay là hoạt động trên phạm vi toàn cầu với doanh thu hàng năm có thể lên tới hàng trăm triệu đô, thậm chí trên 1 tỷ đô.

2. Xu hướng phát triển của Ransomware – Ransomware as a Service

Giai đoạn từ năm 2018 trở về trước, tấn công mã độc Ransomware thường hướng tới đối tượng cá nhân. Do đó, việc xâm nhập, phát tán, lây lan có thể bùng nổ trên diện rộng, thiệt hại nhiều cho cá nhân, nhưng không tác động quá lớn đến các tổ chức

Tuy nhiên, những sự cố gần đây cho thấy các nhóm tấn công đã chuyển hướng và nhắm vào doanh nghiệp nhiều hơn, gây tổn thất nặng nề và yêu cầu tiền chuộc cao hơn.

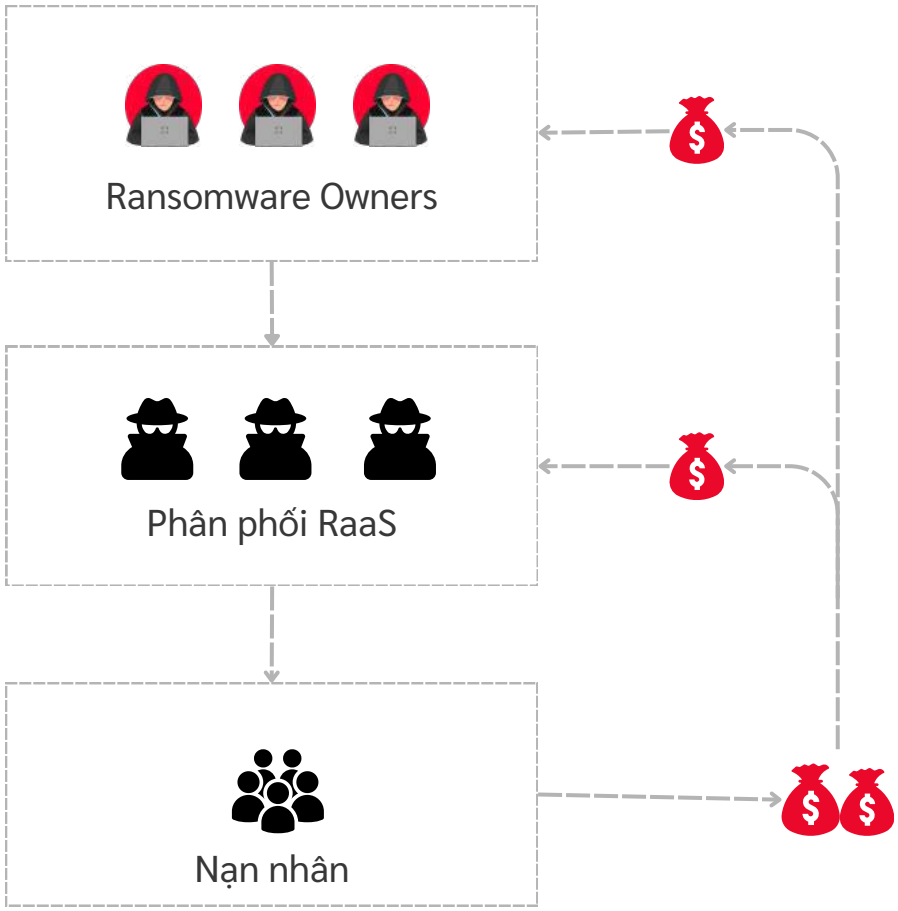
“Ransomware gắn với tấn công có chủ đích APT trở thành mô hình kinh doanh đại lý siêu lợi nhuận, để bất cứ ai có tiền, có ý đồ xấu đều có thể thực hiện tấn công Ransomware”.

- Tại các doanh nghiệp, Ransomware luôn tìm kiếm và mã hóa dữ liệu sao lưu.
- Các nhóm tấn công Ransomware kết hợp phương thức tấn công có chủ đích APT để tìm các điểm yếu quan trọng trong hệ thống sau đó mới kích nổ - tức thực hiện hành vi mã hóa.
- **Thời gian kẻ tấn công ở trong hệ thống rất dài, lên tới 6 tháng đến 1 năm**, do đó rất am hiểu hành vi của tổ chức, chỉ trực chờ thời điểm thích hợp để thực hiện mã hóa dẫn tới hậu quả gây ra là vô cùng khủng khiếp.

Nhìn thấy lợi nhuận, các nhóm tin tặc đã sẵn sàng đầu tư để có được doanh thu cao hơn. Ransomware không còn là mã độc đơn thuần mà đã trở thành một ngành công nghiệp.

So với trước đây, phạm vi và số cuộc tấn công Ransomware đã tăng đột biến và mở rộng hơn rất nhiều. Sự bùng nổ này xuất phát từ sự chuyển đổi từ mô hình truyền thống sang mô hình Ransomware as a service.

- **Mô hình truyền thống:** Ransomware owner (*) cần có nguồn lực, kỹ năng và sự chuẩn bị kỹ càng về hạ tầng ẩn danh trên mạng để chứa các server điều khiển. Sau đó, chúng tổ chức các chiến dịch rà soát, xâm nhập, lây lan, cài cắm, lấy dữ liệu, mã hóa dữ liệu, và tương tác với nạn nhân để đòi tiền chuộc. Có rất nhiều công đoạn và đòi hỏi nhiều kỹ năng, do đó có không nhiều tổ chức có thể thực hiện việc tấn công Ransomware.
- **Mô hình dịch vụ Ransomware as a service (RaaS) - mô hình phân phối:** Các nhóm Ransomware Owner trước đây chuyển sang cung cấp dịch vụ, đảm bảo duy trì hạ tầng Ransomware và cho thuê ra bên ngoài. Họ quảng cáo về hạ tầng, công cụ, để bất cứ ai có tiền, có ý đồ xấu đều có thể thực hiện tấn công Ransomware. Việc tấn công Ransomware trở nên rất đơn giản, và chia sẻ lợi nhuận cao.



Nhìn chung, trên phạm vi toàn cầu, mô hình này đang nở rộ như một trào lưu cho phép rất nhiều các nhóm tấn công nhỏ lẻ thực hiện tấn công Ransomware.

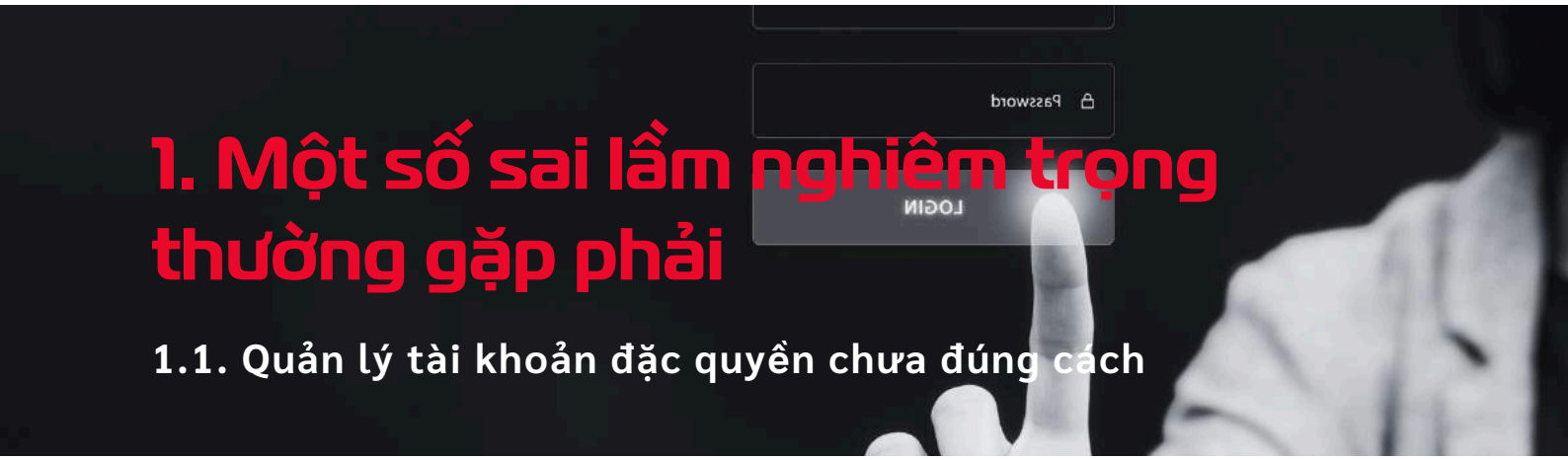
(*): Ransomware owner chỉ các cá nhân hoặc nhóm đứng sau việc phát triển, phát tán và quản lý ransomware

II. Khuyến nghị từ VCS

phòng ngừa và ứng phó với tấn công mã hóa dữ liệu Ransomware

Với sự nở rộ của mô hình Ransomware as a service, việc tấn công Ransomware trở nên dễ dàng hơn bao giờ hết. Đồng thời tấn công Ransomware kết hợp với APT ngày càng tinh vi, nguy hiểm gây thiệt hại lớn cho các doanh nghiệp.

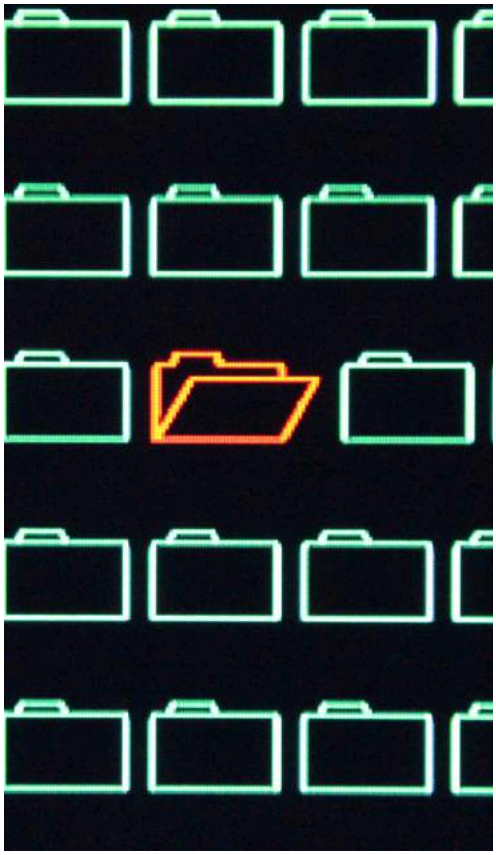
VCS khuyến cáo doanh nghiệp chủ động phòng chống và hạn chế bị tấn công Ransomware thông qua việc: Đầu tư, trang bị cho hệ thống ATTT và Vận hành đúng cách, đặc biệt là câu chuyện vận hành.



1. Một số sai lầm nghiêm trọng thường gặp phải

1.1. Quản lý tài khoản đặc quyền chưa đúng cách

Đây là con đường ngắn nhất và là mục tiêu đầu tiên của kẻ tấn công bởi khả năng tác động rất lớn, ví dụ với tài khoản quản lý toàn bộ hạ tầng ảo hóa. Việc quản lý tài khoản & lưu trữ tài khoản đặc quyền này nhiều doanh nghiệp vẫn đang gặp vấn đề. Doanh nghiệp đang sử dụng tài khoản đặc quyền cho rất nhiều nghiệp vụ, xác thực trên các máy khác, dẫn tới vô tình để lại thông tin mật khẩu trên bộ nhớ của các máy trạm.



Nguy cơ: Kẻ tấn công chiếm tài khoản đặc quyền để dễ dàng xâm nhập, leo thang và tấn công hệ thống.

Khuyến nghị:

- Triển khai các giải pháp quản lý tài khoản đặc quyền (PAM/PIM), theo dõi và ghi lại hoạt động của người dùng trong các phiên làm việc đặc quyền để phát hiện và phản ứng nhanh chóng với các hành vi đáng ngờ.
- Xác định và phân loại tài khoản đặc quyền dựa trên mức độ rủi ro và tầm quan trọng.

- Áp dụng nguyên tắc đặc quyền tối thiểu (Least Privilege): Cấp quyền chỉ đủ để thực hiện công việc cần thiết và không hơn.
- Xác thực đa yếu tố (MFA): Yêu cầu nhiều hình thức xác thực trước khi cấp quyền truy cập.
- Kiểm soát truy cập từ xa: Đảm bảo rằng truy cập từ xa đến tài khoản đặc quyền được bảo mật và kiểm soát chặt chẽ.
- Phản ứng nhanh chóng khi có dấu hiệu bất thường: Thiết lập hệ thống cảnh báo để nhận biết sớm các hoạt động không bình thường và có biện pháp can thiệp kịp thời.
- Rà soát định kỳ các tài khoản có chức năng quản trị để hạn chế tối đa việc lạm dụng leo thang vào các hệ thống khác.
- Loại bỏ các tài khoản không cần thiết hoặc không còn được sử dụng để giảm thiểu điểm yếu có thể bị tấn công.

1.2. Cho phép mở kết nối với các giao thức truy cập từ xa như VPN, RDP thông qua các cổng mặc định dễ nhận biết, không giới hạn thiết bị sử dụng.

Nguy cơ: Kẻ tấn công có thể dò quét ra các dịch vụ kết nối từ xa, từ đó có thể khai thác các lỗ hổng của dịch vụ kết nối từ xa hoặc lợi dụng các tài khoản kết nối để xâm nhập.

Khuyến nghị:

- Thay đổi cổng kết nối mặc định đến RDP, VPN. Mặc định không chia sẻ, hiển thị các thông tin VPN, RDP trên website.
- Hạn chế các user, các thiết bị, IP được phép sử dụng RDP.
- Quy hoạch thiết kế hệ thống mạng chặt chẽ, kiểm soát mọi kết nối giữa các phân vùng mạng khác nhau. Đồng thời rà soát liên tục để đảm bảo không có kết nối bất thường được mở theo nguyên tắc "**Zero Trust Network Access**".

1.3 Cho phép đối tác và các dịch vụ bên thứ ba kết nối vào trong hệ thống của tổ chức mà không có phân quyền, giới hạn truy cập.

Các yêu cầu về việc mở các ứng dụng để kết nối phục vụ sản xuất kinh doanh ngày càng cao, nhưng nhiều doanh nghiệp chưa có chính sách kết nối chặt chẽ dẫn đến cấu trúc mạng ngày càng phẳng tạo điều kiện cho kẻ tấn công dễ dàng có được quyền kết nối và xâm nhập vào hệ thống.

Nguy cơ: Kẻ tấn công có thể tấn công các đối tác, dịch vụ bên thứ ba từ đó kết nối trực tiếp vào trong hệ thống của tổ chức.

Khuyến nghị:

- Áp dụng nguyên tắc đặc quyền tối thiểu cho tất cả các bên, bên thứ ba chỉ được truy cập với quyền tối thiểu để thực hiện nghiệp vụ tương ứng.
- Xem xét triển khai hệ thống kiểm soát truy cập **(Zero Trust Network Access)**, chỉ cho phép truy cập hoặc sử dụng khi có quyền.

1.4 Lỗi lưu trữ mật khẩu: Tài khoản đăng nhập email, VPN hoặc hệ thống quan trọng được lưu trữ trên trình duyệt hoặc môi trường không an toàn

Do quá nhiều mật khẩu, người dùng thường lưu trữ ngay trên file excel, word, hay desktop, lưu mật khẩu trên các trình duyệt, hoặc nhập thông tin trên các biểu mẫu, máy tính không an toàn, khiến mật khẩu rất dễ bị đánh cắp. Trên thực tế, rất nhiều tài khoản đặc quyền đang được rao bán trên chợ đen.

Nguy cơ: Kẻ tấn công lấy mật khẩu được lưu trữ trên trình duyệt để thực hiện tấn công.

Khuyến nghị:

- Không lưu trữ mật khẩu trên trình duyệt.
- Thực hiện sử dụng các phần mềm chuyên dụng để quản lý mật khẩu
- Bổ sung cơ chế xác thực đa nhân tố cho các hệ thống, tài khoản trọng yếu.

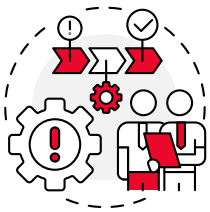
2. Quy trình ứng phó khẩn cấp khi bị tấn công Ransomware

Liên hệ với đơn vị ATTT có uy tín, năng lực để hỗ trợ xử lý sự cố

Giúp doanh nghiệp đánh giá mức độ nghiêm trọng của sự cố, xác định nguồn gốc và cung cấp các biện pháp khắc phục kịp thời.

Phản ứng nhanh

Khoanh vùng, phát hiện phạm vi, đưa ra phương án phản ứng nhanh để cô lập và giảm thiểu thiệt hại về sau, phục vụ việc điều tra sâu & lên phương án xử lý cụ thể.



Điều tra số

Điều tra sâu & đầy đủ tất cả các hành vi, con đường của kẻ tấn công một cách đầy đủ. Nếu không điều tra hết các điểm yếu của hệ thống, sẽ không thể phản ứng và giải quyết vấn đề triệt để. Nhiều doanh nghiệp sau khi bị tấn công đã khôi phục lại hệ thống nhưng vẫn rất yếu, do không nhận diện được phương thức tấn công của kẻ tấn công và chỉ muốn nhanh chóng lấy lại tài sản. Do đó, cần phải điều tra, theo dõi hành vi của tội phạm mạng để nắm bắt phương thức tấn công. Mục tiêu khôi phục hệ thống phải đi kèm với việc điều tra khả năng bị tấn công về sau.

Khắc phục sự cố

Bộ phận ATTT phối hợp với các nhân sự chức năng khác, chung sức khôi phục hệ thống, máy chủ và các ứng dụng trong doanh nghiệp, khắc phục các điểm yếu đã bị kẻ tấn công khai thác để xâm nhập, chiếm quyền điều khiển hệ thống.

Bài học kinh nghiệm

Chỉ ra các vấn đề còn yếu, thiếu để lên kế hoạch củng cố ATTT cho doanh nghiệp trong trung hạn và dài hạn

3. Phương án tiếp cận trước, trong và sau khi xảy ra tấn công

Bắt buộc **Ưu tiên** **Khuyến nghị**

Quản lý thật tốt các tài khoản đặc quyền

Đây là con đường ngắn nhất và cũng là mục tiêu đầu tiên của kẻ tấn công để xâm nhập vào hệ thống của doanh nghiệp. Vì vậy, doanh nghiệp nên có các biện pháp rà soát, lưu trữ tài khoản đặc quyền, quản lý kênh kết nối phù hợp và thường xuyên bằng các giải pháp kiểm soát truy cập (Zero Trust Network Access) và các giải pháp quản lý tài khoản đặc quyền (PAM/PIM)

Thực hiện việc tầm soát định kỳ (Compromise Assessment) theo thời gian 3 tháng - 6 tháng

Kẻ tấn công xâm nhập và ẩn mình trong hệ thống một thời gian rất lâu trước khi thực hiện hành vi mã hóa dữ liệu (trung bình 200 ngày - theo nhận định của chuyên gia VCS). Bởi vậy doanh nghiệp cần thực hiện các giải pháp rà quét định kì để phát hiện sớm bất thường, phát hiện sớm để phản ứng sớm, từ đó phản ứng kịp thời trong giai đoạn đầu - doanh nghiệp đã bị xâm nhập nhưng ngăn chặn được mã hóa dữ liệu.

Triển khai các giải pháp Giám sát ATTT 24/7

Đây là phương án lý tưởng nhất cho doanh nghiệp để phát hiện và phản ứng sớm với các cuộc tấn công vào hệ thống trước khi xảy ra các thiệt hại nặng nề.

3. Phương án tiếp cận trước, trong và sau khi xảy ra tấn công

Để có thể có phương án đầu tư phù hợp nhất, Doanh nghiệp có thể liên hệ và tìm kiếm sự hỗ trợ từ các chuyên gia của VCS để được tư vấn về chiến lược đầu tư dài hạn phù hợp với hiện trạng từng doanh nghiệp.

Bắt buộc **Ưu tiên** **Khuyến nghị**

Chuẩn bị kịch bản giả định khi sự cố xảy ra

Doanh nghiệp rất bối rối khi sự cố xảy ra, do không có 1 framework cụ thể để xử lý và phản ứng nhanh để có phương án phối hợp tối ưu. Do đó cần đưa vào 1 số yếu tố cho kịch bản ứng cứu với sự phối hợp của không chỉ đội ngũ an ninh bảo mật như sau:

- Đội ngũ truyền thông: Truyền thông xử lý khủng hoảng để đảm bảo uy tín doanh nghiệp
- Đội ngũ hạ tầng hệ thống: Dựng lại hệ thống ứng dụng "1 cách an toàn" thay vì nhanh chóng khôi phục "nhưng không đảm bảo"
- Đội ngũ an ninh bảo mật, điều tra, khôi phục hệ thống, máy chủ, ứng dụng đều cùng phải chung sức khi xảy ra vấn đề

Giải pháp sao lưu và phục hồi toàn diện

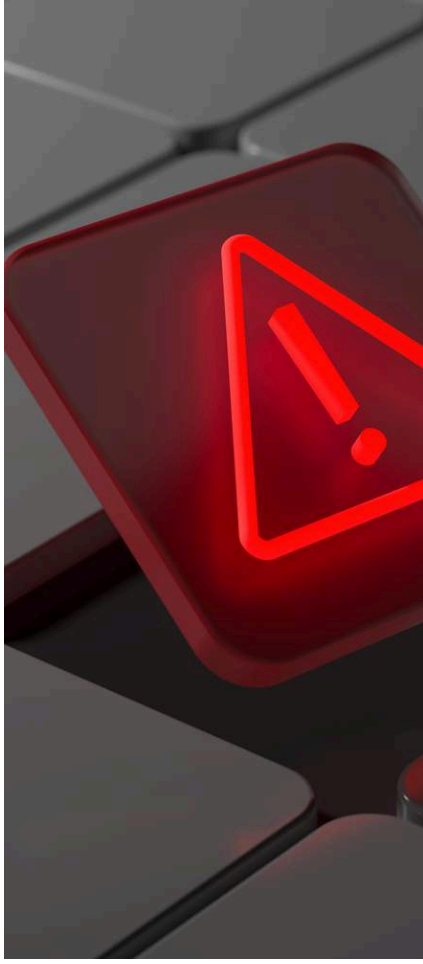
Hệ thống sao lưu và phục hồi phải tách biệt và không được kết nối với các hệ thống khác trong mạng.

Nhận thông tin cảnh báo sớm thông qua các giải pháp như Threat Intelligence và các giải pháp quản lý các bề mặt tấn công (External Attack Surface Management) để nhận biết và phản ứng sớm với các chiến dịch tấn công xâm nhập, tấn công mã hoá dữ liệu đang xảy ra trên môi trường mạng.

III.
PHỤ LỤC

viettel security

1. Kịch bản tấn công **mã hóa dữ liệu hạ tầng ảo** tại Việt Nam

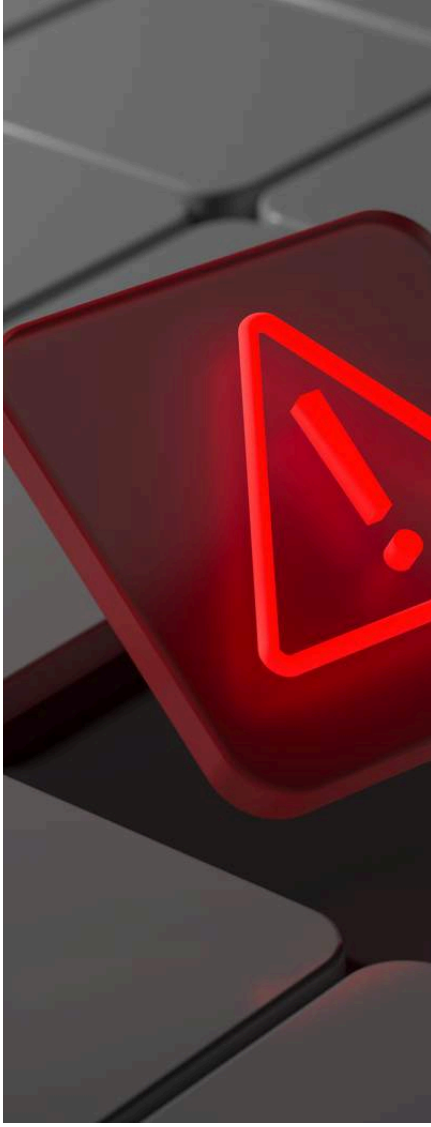


Bước 1: Kẻ tấn công truy cập vào mạng nội bộ

- Mã độc được cài vào trong mạng nội bộ thông qua email, websites lừa đảo, từ USB,...
- Thông qua bruteforce hoặc lấy được các tài khoản đăng nhập hệ thống kết nối từ xa bị đánh cắp (Compromised Account) để truy cập vào mạng nội bộ.
- Thông qua khai thác lỗ hổng trên các hệ thống public, kẻ tấn công cài webshell và leo thang vào bên trong mạng nội bộ.

Bước 2: Leo quyền

Khi kẻ tấn công có quyền truy cập vào một máy trong mạng nội bộ, kẻ tấn công sẽ cố gắng leo quyền để tấn công.



Bước 3: Kẻ tấn công tìm cách truy cập được vào vùng mạng quản trị.

Sau khi leo quyền, kẻ tấn công thực hiện tấn công để truy cập vào vùng mạng chứa hệ thống quản trị ảo hóa bằng nhiều hình thức như:

- Thông qua việc cho phép máy trạm truy cập được vùng mạng quản trị.
- Thông qua việc sử dụng chung tài khoản AD cho máy tính truy cập vùng mạng quản trị.
- Thông qua việc không xác thực 2 bước khi truy cập vào vùng mạng quản trị.

Bước 4: Kẻ tấn công chiếm quyền truy cập vào hệ thống quản trị ảo hóa vCenter

- Khi kẻ tấn công ở trong vùng mạng quản trị, kẻ tấn công tận dụng các điểm yếu sau để có thể chiếm quyền truy cập vào hệ thống quản trị vCenter:
- Thông qua việc khai thác lỗ hổng chiếm quyền điều khiển trên hệ thống quản trị vCenter như: CVE-2022-31680, CVE-2021-22005, CVE-2021-21985, CVE-2021-21972,..
- Thông qua việc ăn cắp tài khoản quản trị được lưu trên các hệ thống trung gian.
- Sau đó, kẻ tấn công thực hiện bật ssh vào ESXi hoặc thay đổi mật khẩu ssh của ESXi.

Bước 5: Kẻ tấn công thực hiện mã hóa toàn bộ các hệ thống ảo hóa và đòi tiền chuộc

Kẻ tấn công truy cập ssh vào ESXi, thực hiện tắt máy ảo và chạy công cụ mã hóa toàn bộ các máy ảo.

viettel security

2. Một số câu hỏi thường gặp

Câu 1: Có nên trả tiền khi bị tấn công Ransomware hay không?

Trả lời: Việc trả tiền hay không phụ thuộc vào chính doanh nghiệp, tuy nhiên, VCS khuyến nghị không nên trả tiền. Doanh nghiệp cần cân nhắc:

- Đã có những trường hợp thực tế, doanh nghiệp trả tiền xong nhưng kẻ tấn công không gửi lại công cụ giải mã hoặc mã đã hết hạn, mã không hoạt động,... Không có một cam kết chắc chắn nào về việc doanh nghiệp trả tiền - nhận tool giải mã thành công.
- Khi thực hiện trả tiền cho tội phạm mạng doanh nghiệp đã tạo động lực cho các nhóm tấn công thực hiện hành vi tội phạm nhiều hơn để kiếm tiền nhiều hơn, more money - more motivation.

Câu 2: Ransomware có thể được phát hiện trước khi bị tấn công không?

Trả lời: Dữ liệu mã hóa là giai đoạn cuối cùng trong cuộc tấn công Ransomware. Trước đó, chúng ta có giai đoạn "cửa sổ" để rà soát định kỳ, nhận biết sớm các dấu hiệu và lên kế hoạch phản ứng.

Câu 3: Làm thế nào để xử lý sự cố tấn công mã độc tống tiền đối với các tổ chức không có hệ thống giám sát ATTT

Trả lời: Nếu không có hệ thống giám sát ATTT, doanh nghiệp có thể sử dụng dịch vụ để kiểm tra định kỳ như dịch vụ đánh giá xâm nhập hệ thống.

IV. Kết luận

Các nhóm tội phạm mạng đang biến tấn công Ransomware trở thành một mô hình kinh doanh siêu lợi nhuận - "Ransomware as a service". Với vốn đầu tư lớn có được từ các khoản tiền chuộc của doanh nghiệp, kẻ tấn công liên tục nghiên cứu và tái đầu tư nhằm thu lại những khoản lợi nhuận cao hơn.

Còn doanh nghiệp đang làm gì để bảo vệ ATTT của chính mình?
Đây là câu hỏi lớn mà mọi doanh nghiệp đều cần phải trả lời nếu muốn bảo vệ tên tuổi, uy tín, tài sản và cả sự sống còn của doanh nghiệp.

Thông qua tài liệu hướng dẫn về Ransomware, Công ty An ninh mạng Viettel hy vọng đã mang đến những kiến thức cơ bản và toàn diện về loại hình tội phạm mạng nguy hiểm bậc nhất hiện nay.

An ninh mạng là cuộc chiến đối kháng không ngừng nghỉ giữa 2 thế lực tấn công và phòng thủ về cả tri thức và kỹ thuật. Chúng tôi sẵn sàng tư vấn và đồng hành cùng doanh nghiệp trong hành trình chống lại tội phạm mạng và thúc đẩy sự phát triển an toàn của doanh nghiệp.

Công ty An ninh mạng Viettel

Về chúng tôi

Công ty An ninh mạng Viettel (Viettel Cyber Security - VCS) trực thuộc Tập đoàn Công nghiệp - Viễn thông Quân đội (Viettel), thực hiện nghiên cứu sâu rộng và phát triển các giải pháp bảo mật thông tin, cung cấp các dịch vụ và sản phẩm an ninh mạng nhằm bảo vệ tài sản số của hạ tầng trọng yếu quốc gia và các tổ chức, doanh nghiệp trong nước và quốc tế.

viettel security

Đối tác cung cấp dịch vụ ATTT số 1 Việt Nam

https://viettelcybersecurity.com/