ĐIỀU TRA THẤT THOÁT TÀI SẢN QUA EMAIL

(Nghiêm cấm đăng tải trên internet dưới mọi hình thức)

1. Giới thiệu

Các giám đốc điều hành của MINAF (Minerías Alcazar y Ferrán, công ty khai thác quốc tế với doanh thu hàng năm trên 40 triệu Euro) tuyệt vọng nhờ bạn giúp đỡ vì họ gặp một vấn đề: 100 nghìn Euro đã biến mất khỏi tài khoản ngân hàng của họ.

Sau khi phỏng vấn CEO và CFO của MINAF, bạn thu thập được một số thông tin như sau:

- MINAF vài tháng nay đang đàm phán với Coltranistan (một nước thuộc Cộng hòa liên bang Xô Viết ở Trung Đông) để triển khai hoạt động khai thác Coltan, có giá trị kinh tế lên tới hàng chục triệu Euro.
- Cả 2 công ty gần như đạt được các thỏa thuận liên quan. Một cuộc gặp mặt tại Estanbul vào ngày 07/06/2019 nhằm kết thúc vụ đàm phán này, vì vậy CEO của MINAF, Abelardo Alcazar, đã bay tới đó vào buổi sáng ngày 07/06/2019.
- Khoảng 17 giờ cùng ngày, CFO của MINAF, Alfonso Ferran, nhận được email từ CEO, yêu cầu chuyển khoản đến một vài ngân hàng quốc tế với số tiền lên tới 100 nghìn Euro.
- Sau cuộc trao đổi ngắn qua Email, Alfonso Ferran đã thực hiện chuyển khoản vào lúc 17 giờ 30 phút.
- Abelardo Alcazar trở về Tây Ban Nha vào khoảng 13 giờ ngày 09/06/2019 và gọi cho Alfonso Ferran. Alfonso Ferran nói với anh ta về những lo ngại trong việc chuyển khoản, và Abelardo Alcazar hoàn toàn phủ nhận việc mình đã ra lệnh chuyển khoản đến các ngân hàng này.
- Thiết bị di động của Abelardo Alcazar đã ngừng hoạt động vào khoảng 20 giờ 30 phút ngày 07/06/2019, ngay sau khi gửi Email cho Alfonso Ferran để thông báo cuộc đàm phán đã thành công.
- Nghi ngờ đây là một vụ lừa đảo, vi phạm an toàn thông tin, vì vậy, họ đã nhờ bạn làm sáng tỏ sự thật.

2. Các thông tin được cung cấp

Các hệ thống Công nghệ Thông tin của MINAF bao gồm:

- Người dùng cuối sử dụng Windows 7 (SP1, 64 bit)
- Một vài máy chủ Windows Server 2008R2, bao gồm:
    - Một Domain Controller
    - Một File Server
    - Một máy chủ Microsoft Exchange 2010 để gửi và nhận Email. Máy chủ Exchange có các dịch vụ OWA và ActiveSync được kích hoạt và có thể truy cập thông qua Internet (cần thiết cho việc sử dụng mọi nơi).
    - Các giám đốc điều hành (bao gồm CEO và CFO) được cấp riêng thiết bị di động (Samsung Galaxy S9)

Hệ thống Công nghệ Thông tin của MINAF luôn tuân thủ các cấu hình bảo mật:

- Mọi máy chủ và máy tính người dùng cuối đều trang bị phần mềm chống virus và luôn cập nhật các bản vá bảo mật.
- Ngoài ra, các chính sách bảo mật liên quan đến mật khẩu (được thực hiện thông qua GPO): độ dài mật khẩu phải tối thiểu 10 ký tự với các yêu cầu mật khẩu phức tạp được kích hoạt.

3. Các chứng cứ thu thập được:

Quản trị hệ thống của MINAF cung cấp cho chúng ta một số chứng cứ:

- Tập tin **MINAF-PC1.zip** (CFO của MINAF, Alfonso Ferran)
    - MINAF-PC1_triage.zip – dữ liệu trên máy tính
    - MINAF-PC1-Outlook.zip – thư mục Outlook
- Tập tin **MINAF-PC2.zip** (CEO của MINAF, Abelardo Alcazar)
    - MINAF-PC2_triage.zip – dữ liệu trên máy tính
    - MINAF-PC2-Outlook.zip – thư mục Outlook
- Tập tin **CORREO.zip**:
    - MINAF-CORREO_triage.zip – dữ liệu ưu tiên

- CORREO_CAS_LogFiles.zip – các log Exchange CAS (Client Access Server)
- CORREO-MessageTracking.csv – bảng theo dõi các tin nhắn trong Exchange
- CORREO-EventHistory_Abelardo_Alcazar.txt – lịch sử sự kiện của Abelardo Alcazar (CEO của MINAF)
- CORREO-EventHistory_Alfonso_Ferran.txt – lịch sử sự kiện của Alfonso Ferran (CFO của MINAF)
- CORREO-Buzon_Abelardo_Alcazar.pst – Hòm thư được trích xuất của Abelardo Alcazar
- CORREO-Buzon_Alfonso_Ferran.pst – Hòm thư trích xuất của Alfonso Ferran

- Mã băm của tất cả chứng cứ nằm ở tập tin **hashes.txt**

Lưu ý 1: bất kỳ chứng cứ nào tìm thấy trước ngày 01/06/2019 đều không liên quan đến vụ việc này.

Lưu ý 2: đáp án không phân biệt chữ hoa và chữ thường và phải được trả lời ở dạng văn bản thô.

Lưu ý 3: Nội dung Email được viết bằng tiếng Tây Ban Nha.

Lưu ý 4: Định dạng flag: inseclab{ANSWER}

4. Mục tiêu

Trả lời các câu hỏi sau nhằm giúp MINAF tìm ra kẻ đã lấy tiền của họ:

1. Một trong những việc đầu tiên của điều tra viên chính là kiểm tra mã băm của các chứng cứ mà MINAF cung cấp. Một trong các chứng cứ được cung cấp gặp vấn đề, đó là tập tin nào?
2. Sử dụng tập tin MINAF-PC2-Outlook.zip, xác định có tổng cộng bao nhiêu Email được gửi từ tài khoản abelardo.alcazar trong khoảng thời gian từ 02/06/2019 đến 07/06/2019?

3. Sử dụng tập tin MINAF-PC2-Outlook.zip và cho biết tên hãng điện thoại mà Abelardo Alcazar sử dụng.
4. Kiểm tra sơ bộ tập tin MINAF-Outlook-PC1.zip, chúng ta phát hiện tập tin này đã bị …? (Gợi ý, đây là 1 từ tiếng Anh diễn tả trạng thái của tập tin đang sử dụng)
5. Vào ngày 07/06/2019, có một vài Email được gửi với tiêu đề (subject) chứa từ khóa "COBALTO". Hãy cho biết Email đầu tiên được gửi vào thời gian nào? (Ghi chú, trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS)
6. Có bao nhiêu Email THẬT SỰ được gửi bởi tài khoản abelardo.alcazar từ ngày 02/06/2019 đến ngày 07/06/2019? (Gợi ý, đừng đếm các Email yêu cầu xóa từ xa – remotewipe)
7. Vào ngày 07/06/2019, có một vài yêu cầu chuyển khoản ngân hàng được yêu cầu. Hãy cho biết số tài khoản? (Định dạng: sắp xếp theo thứ tự từ bé đến lớn, cách nhau bởi dấu ',' và không có khoảng trắng)
8. Vào ngày 07/06/2019, có một vài Email được gửi với tiêu đề (subject) chứa từ khóa "COBALTO". Bạn hãy cho biết thời gian chính xác mà lá thư đầu tiên được gửi bắt đầu từ lúc soạn thư? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS. (Gợi ý, tùy thuộc vào chứng cứ mà bạn sử dụng, số giây có thể sai số trong khoảng "+1/-1", vì vậy hãy bình tĩnh)
9. Mỗi Exchange email đều có một trường nào đó duy nhất cho phép máy chủ email xác định chúng. Hãy cho biết tên của trường đó? (Gợi ý, trường đó được hiển thị ở cả 2 vị trí MessageTracking và EventHistoryDB)
10. Cho biết giá trị của trường đó đối với Email đầu tiên được gửi bởi tài khoản abelardo.alcazar vào ngày 07/06/2019 với tiêu đề (subject) chứa từ khóa "COBALTO"? (Lưu ý, bỏ dấu "-" trong câu trả lời)
11. Email khá là quan trọng. Hãy cho biết giá trị của trường DocumentId?
12. Email này đã hoàn thành nhiệm vụ của nó. Hãy cho biết thời gian mà Email này được xóa? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS.
13. Thật buồn cười nhưng Email đó không hoàn toàn bị xóa sạch ngay lần đầu tiên nó bị xóa. Bạn có thể đoán được thời gian mà Email này chắc chắn bị xóa khỏi

hộp thư của người dùng không? Trả lời thời gian múi giờ UTC+0, định dạng HH:MM:SS.

14. Email này (và các email liên quan) đã thu hút được rất nhiều sự chú ý. Nhưng, nó thực sự đến từ đâu? Các tùy chọn: Outlook, Mobile, ECP, OWA, PigeonCarrier.
15. Abelardo Alcazar chỉ gửi 1 email duy nhất vào ngày 07/06/2019. Anh ấy đã gửi nó khi nào?
16. Điện thoại của Abelardo Alcazar có DeviceID là bao nhiêu?
17. Nếu quan sát log kỹ hơn, ta có thể thấy có một cái gì đó cố gắng trông giống như một chiếc Android nhưng đã thất bại thảm hại. Hãy cho biết giá trị User-Agent đang được sử dụng để kết nối tới Exchange?
18. Kẻ tấn công không phải bắt đầu tấn công vào hôm nay. Sau khi trả lời được các câu hỏi trước đó, vậy thì lần đầu tiên bạn nhìn thấy địa chỉ IP đó trong log của CAS Exchange là khi nào? Trả lời thời gian múi giờ UTC+0, định dạng YYYY-MM-DD HH:MM:SS.
19. Bằng một cách nào đó mà kẻ tấn công có được tài khoản của abelardo.alcazar. Bạn hãy cho biết lần đầu tiên mà kẻ tấn công đăng nhập thành công vào Exchange Server? Trả lời thời gian múi giờ UTC+0, định dạng YYYY-MM-DD HH:MM:SS. (Lưu ý, chúng tôi định nghĩa "đăng nhập thành công" tính từ lúc gói tin đầu tiên được gửi đi sau khi chứng thực thành công)
20. Kẻ tấn công đã thử rất nhiều cách để có thể vào được tài khoản abelardo.alcazar… nhưng cuối cùng, các kỹ thuật cũ luôn thành công. Bạn hãy cho biết tên miền được sử dụng để lừa đảo Abelardo Alcazar?
21. Với tất cả các chứng cứ thu thập được, ta có thể kết luận MINAF đã gặp phải cuộc tấn công có tên … (Gợi ý, chỉ 3 ký tự)