TRUNG TÂM ỨNG CỨU KHẨN CẤP KHÔNG GIAN MẠNG VIỆT NAM

VIETNAM CYBERSECURITY EMERGENCY RESPONSE TEAMS/COORDINATION CENTER

# VNCERT/CC

# SỔ TAY ỨNG CỨU SỰ CỐ

## Sự cố giả mạo ( Phishing )


Tầng 5, 115 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội

ir@vncert.vn

0869 100 317

https://vncert.vn/

# MỤC LỤC



## DANH SÁCH CÁC HÌNH

# 1. Giới thiệu

## 1.1. Bối cảnh

An toàn thông tin là các hoạt động bảo vệ tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin và dữ liệu được xử lý, lưu trữ và truyền đạt bằng các phương tiện điện tử hoặc tương tự, bảo vệ thông tin và các hệ thống liên quan khỏi mối đe dọa bên ngoài hoặc bên trong thông qua sự liên kết từ con người, quy trình và công cụ.

Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính bí mật, tính toàn vẹn hoặc tính sẵn sàng.

Với các công nghệ củng cố cơ sở hạ tầng Công nghệ thông tin và các hệ thống liên quan ngày càng tiến bộ, tội phạm mạng cũng đẩy mạnh khai thác công nghệ mới để tiến hành tấn công mạng với mục đích giả mạo, lừa đảo, phạm tội... Nhiều tổ chức có quy mô khác nhau và từ tất cả các ngành đã bị tấn công mạng rất nhiều trong các năm qua. Các mối đe dọa được biết đến đã sử dụng các phương pháp tấn công nâng cao để thâm nhập vào các hệ thống mạng với hình thức tinh vi hơn để tránh bị phát hiện.

## 1.2. Mục tiêu

Sổ tay ứng cứu sự cố mô tả quá trình cần thiết để quản lý các sự cố trên không gian mạng, cùng với các phản hồi và cách giải quyết để ngăn chặn hoặc hạn chế thiệt hại có thể gây ra. Việc áp dụng sổ tay sẽ giúp giảm phạm vi, tác động và mức độ nghiêm trọng của các sự cố trên mạng.

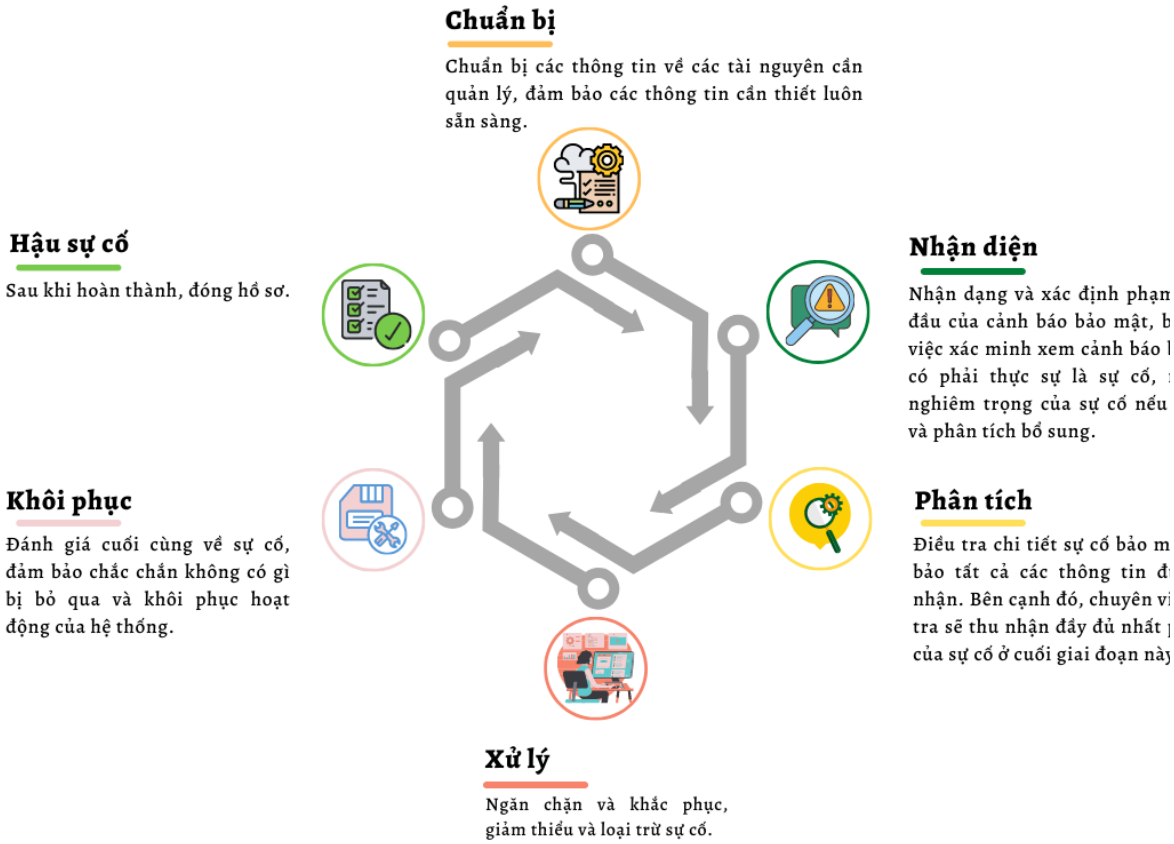
Mỗi loại sự cố sẽ có một sổ tay tương ứng, cho phép người thực hiện theo phương pháp có cấu trúc để xác thực và trả lời từng cảnh báo bảo mật duy nhất. Quy trình ứng cứu sự cố sẽ bao gồm việc xác thực cuộc tấn công, hiểu được tác động và xác định phương pháp ngăn chặn tốt nhất. Quá trình khắc phục kết thúc bằng việc ngăn chặn và loại bỏ cuộc tấn công.

# 2. Quy trình ứng cứu sự cố

Liên hệ Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (Trung tâm VNCERT/CC) để được hỗ trợ trong việc ứng phó với các sự cố mạng tại **ir@vncert.vn** hoặc **+84869100317.**

Đây là Sổ tay ứng cứu sự cố cho **Sự cố giả mạo (Phishing).** Để xem phiên bản mới nhất của Sổ tay, vui lòng truy cập: https://vncert.vn/

## 2.1. Tóm tắt quy trình




*Hình 1: Mô tả các bước của Sổ tay*

## 2.2. Giai đoạn 1: Chuẩn bị

**Tạo và duy trì các danh sách về:** các domain thuộc sở hữu của tổ chức; những người có thể đăng ký domain của tổ chức.

**Tạo các mẫu email:**

- Thông báo cho tất cả nhân viên về chiến dịch lừa đảo đối với tổ chức;

- Liên hệ với Cơ quan điều phối quốc gia nhằm báo cáo và gỡ bỏ domain độc hại (VNCERT/CC, NCSC, v.v.);

- Thông báo cho bên thứ 3 có hành động chống lại lừa đảo (Microsoft, FedEx, Apple, v.v.).

**Thực hiện và đảm bảo:**

- Áp dụng các giải pháp chống phần mềm chống mã độc/chống spam/chống giả mạo.

- Người dùng biết cách báo cáo giả mạo (cách thức nhận biết, nơi báo cáo).

- Phát hiện các tệp tài liệu (documents: docx, xlsx, pptx,...) tạo ra các tiến trình: PowerShell, CMD, WMI, MSHTA,…

- Phát hiện các tệp đính kèm có khả năng là mã độc: Exe, psl, sh, batch/cmd, lnk, dll,…

**Tiến hành diễn tập:** sau khi thực hiện áp dụng sổ tay, định kỳ ít nhất một năm một lần.

**Theo dõi thông tin tình báo (threat intelligence):**

- Các mối đe dọa đối với tổ chức, ngành.

- Các kiểu tấn công phổ biến.

- Rủi ro và lỗ hổng mới phát hiện.

**Bảo đảm quyền truy cập vào các Sổ tay sự cố mất an toàn thông tin vào bất kỳ lúc nào:**

- Sự cố giả mạo (Phishing).

- Sự cố mã hóa phần mềm, dữ liệu, thiết bị (Ransomware).

- Sự cố mã độc (Malware).

- Sự cố nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu (Eavesdropping).

- Sự cố phá hoại thông tin, dữ liệu, phần mềm (DeOS).

- Sự cố thay đổi giao diện (Deface).

- Sự cố truy cập trái phép, chiếm quyền điều khiển (Hijacking).

- Sự cố tấn công tổng hợp sử dụng nhiều hình thức.

- Sự cố từ chối dịch vụ (DDoS/DoS).

**Liệt kê danh sách các tài nguyên và cơ quan chủ quản:**

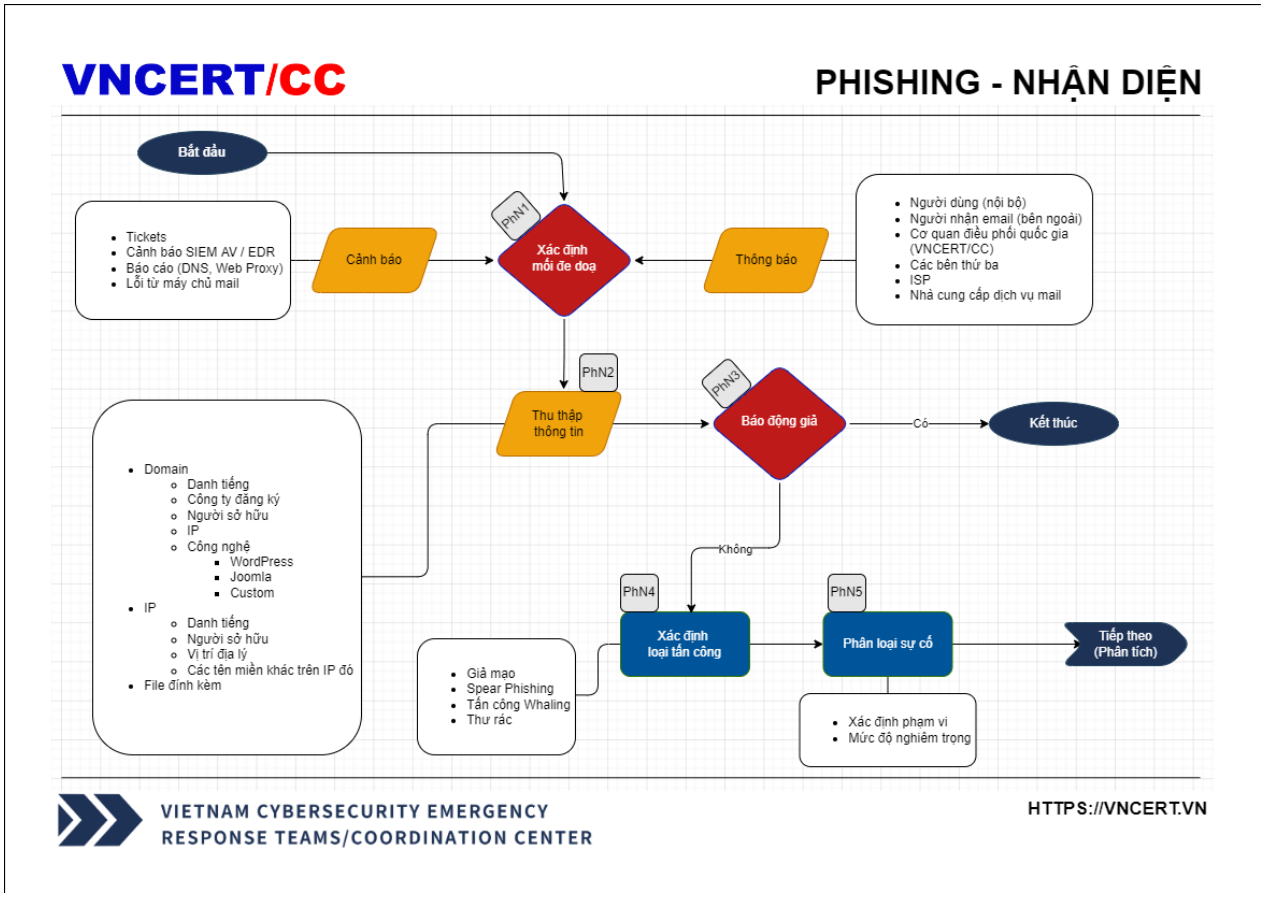
- Tài nguyên của khách hàng: cơ quan chủ quản, thông tin liên lạc, các hành động được ủy quyền.

- Tài nguyên của tổ chức: người vận hành, thông tin liên lạc, các hành động được ủy quyền.

**Các loại tài nguyên cần liệt kê:** Endpoints, máy chủ, thiết bị mạng, thiết bị bảo mật/an toàn, phạm vi mạng (công khai; nội bộ; PN: nhân viên, đối tác, khách hàng).

## 2.3. Giai đoạn 2: Nhận diện

Giai đoạn nhận diện bắt đầu với việc xác định phạm vi ban đầu của một cảnh báo bảo mật:




*Hình 2: Quy trình nhận diện*

### Xác định mối đe doạ

- Cảnh báo: Cảnh báo được tạo ra bởi các hệ thống khác nhau của nhóm Security/SOC. Các nguồn cảnh báo chủ yếu đến từ: Ticket, SIEM Anti-virus / EDR, báo cáo, DNS, Web Proxy, lỗi từ máy chủ mail.

- Thông báo: Thông báo đến từ các nguồn bên ngoài, thường qua email, tin nhắn hoặc điện thoại. Các nguồn thông báo chủ yếu đến từ: người dùng (nội bộ), người nhận email (bên ngoài), các bên thứ ba, ISP, nhà cung cấp dịch vụ mail.

### Thu thập thông tin

Các thông tin cần thu thập về mục tiêu:

- Domain: danh tiếng, công ty đăng ký, người sở hữu, IP, Công nghệ của trang web (WordPress, Joomla, trang tùy chỉnh)

- IP: danh tiếng, người sở hữu, vị trí địa lý, các domain khác trên IP đó.

- Các file đính kèm.

**Xác minh sự cố**

Kết hợp với một chuyên gia SOC: kiểm tra kỹ dữ liệu trước đó, loại trừ báo động giả.

**Xác định loại tấn công**

Xác định loại tấn công thuộc loại nào:

- Giả mạo: trang web của công ty, thương hiệu nổi tiếng (ngân hàng: Vietcombank, VPBank, v.v…), các đơn vị vận chuyển (VNPost, Viettel, Giao hàng nhanh, v.v...), webmail,…

- Spear Phishing.

- Whaling Attack.

- Thư rác.

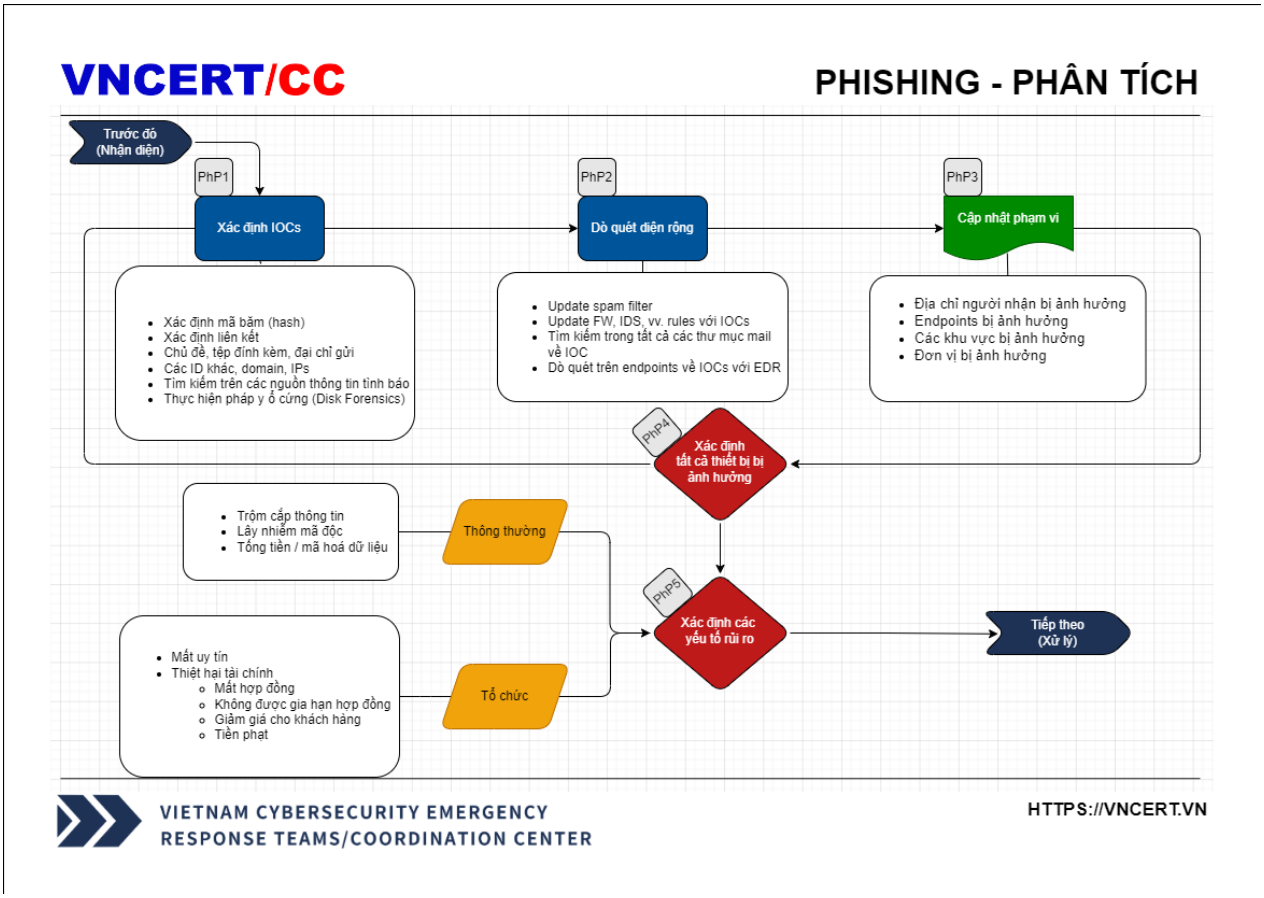
**Phân loại sự cố**

- Xác định mức độ nghiêm trọng: nội dung giả mạo, ảnh hưởng tài chính, mất dữ liệu.

- Phạm vi (số người): nhận được tin nhắn, mở các tệp đính kèm, nhấp vào các liên kết, thông tin đã gửi.

## 2.4. Giai đoạn 3: Phân tích

Giai đoạn này xác định phạm vi, mức độ nghiêm trọng của sự cố:




*Hình 3: Quy trình phân tích*

**Xác định IOCs**

- Xác định mã băm (hash): VirusTotal, Hybrid Analysis.

- Xác định liên kết: VirusTotal, Hybrid Analysis, URLScan.

- Chủ đề, tệp đính kèm, địa chỉ gửi

- Các ID khác, domain, IPs: VirusTotal, Hybrid Analysis, Talos Intelligence.

- Tìm kiếm trên các nguồn thông tin tình báo: VirusTotal, Hybrid Analysis, Talos Intelligence.

- Thực hiện pháp y ổ cứng (Disk Forensics) trên thiết bị của người nhận.

**Dò quét diện rộng**

- Update spam filter.

- Update FW, IDS, vv. rules với IOCs.

- Tìm kiếm trong tất cả các thư mục mail về IOCs.

- Dò quét trên endpoints về IOCs với EDR.

**Cập nhật phạm vi sự cố**

Cập nhật danh sách:

- Địa chỉ người nhận bị ảnh hưởng.

- Endpoints bị ảnh hưởng.

- Các khu vực bị ảnh hưởng.

- Đơn vị bị ảnh hưởng.

**Xác định các thiết bị bị ảnh hưởng**

Nếu đội điều tra tìm thấy dấu vết của tấn công hoặc IOC mới => quay trở lại bước **Xác định IOC**.

- Khi đã hoàn thành bước này, ta cần xác định tất cả các: host, mailbox.

- Và điều tra tất cả: URL, domain, IP, cổng (Port), các tập tin, hash.

- Đã thu thập được ở các bước trên.

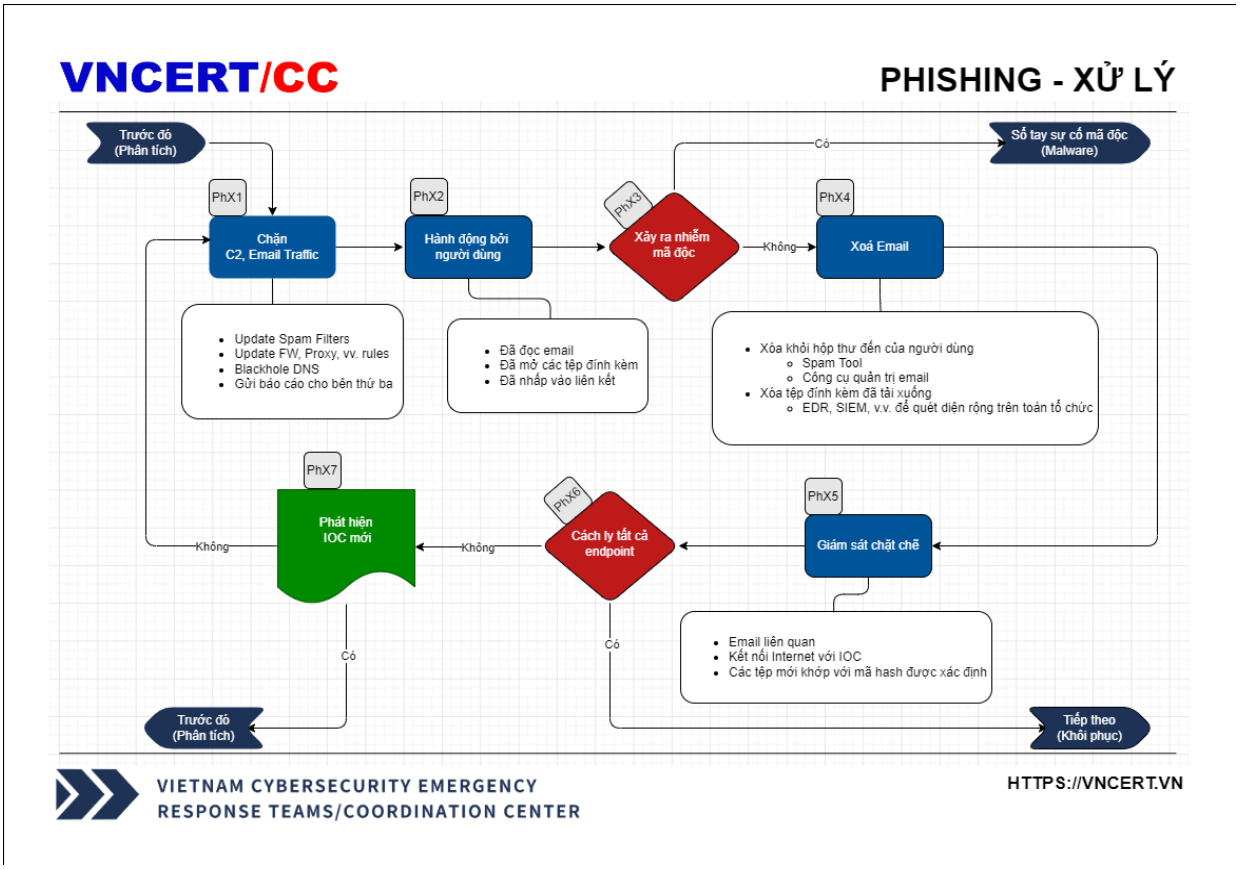
**Xác định các yếu tố rủi ro**

- Thông thường: trộm cắp thông tin, lây nhiễm mã độc, tống tiền / mã hoá dữ liệu.

- Tổ chức: mất uy tín, thiệt hại tài chính, mất hợp đồng, không được gia hạn hợp đồng, phạt / giảm giá.

## 2.5. Giai đoạn 4: Xử lý

Giai đoạn này liên quan đến việc điều tra chi tiết sự cố, đảm bảo tất cả các thông tin đã được phát hiện. Bên cạnh đó, chuyên viên điều tra sự cố sẽ ghi nhận pham vi cuối cùng của sự cố ở giai đoạn này:




*Hình 4: Quy trình xử lý*

### Chặn

- Update Spam Filters.

- Update FW, Proxy, vv. Rules.

- Blackhole DNS.

- Gửi báo cáo cho bên thứ ba: cơ quan điều phối quốc gia, Google Safe Browsing, nhà cung cấp bộ lọc web,…

### Xác minh hành động của người dùng

- Đã đọc email.

- Đã mở các tệp đính kèm.

- Đã nhấp vào liên kết.

**Sự cố mã độc**

- Nếu có các tệp đính kèm độc hại đã được mở, chúng ta cần giả sử các endpoint đã bị nhiễm mã độc.

- Tiếp tục với **Sổ tay sự cố mã độc (Malware).**

**Xóa email**

- Xóa khỏi hộp thư đến của người dùng: Spam Tool, công cụ quản trị email.

- Xóa tệp đính kèm đã tải xuống: EDR, SIEM, v.v. để quét diện rộng trên toàn tổ chức.

**Giám sát chặt chẽ**

Giám sát các: Email liên quan, kết nối Internet với IOC, các tệp mới khớp với mã hash được xác định.

**Cách ly các Endpoints**

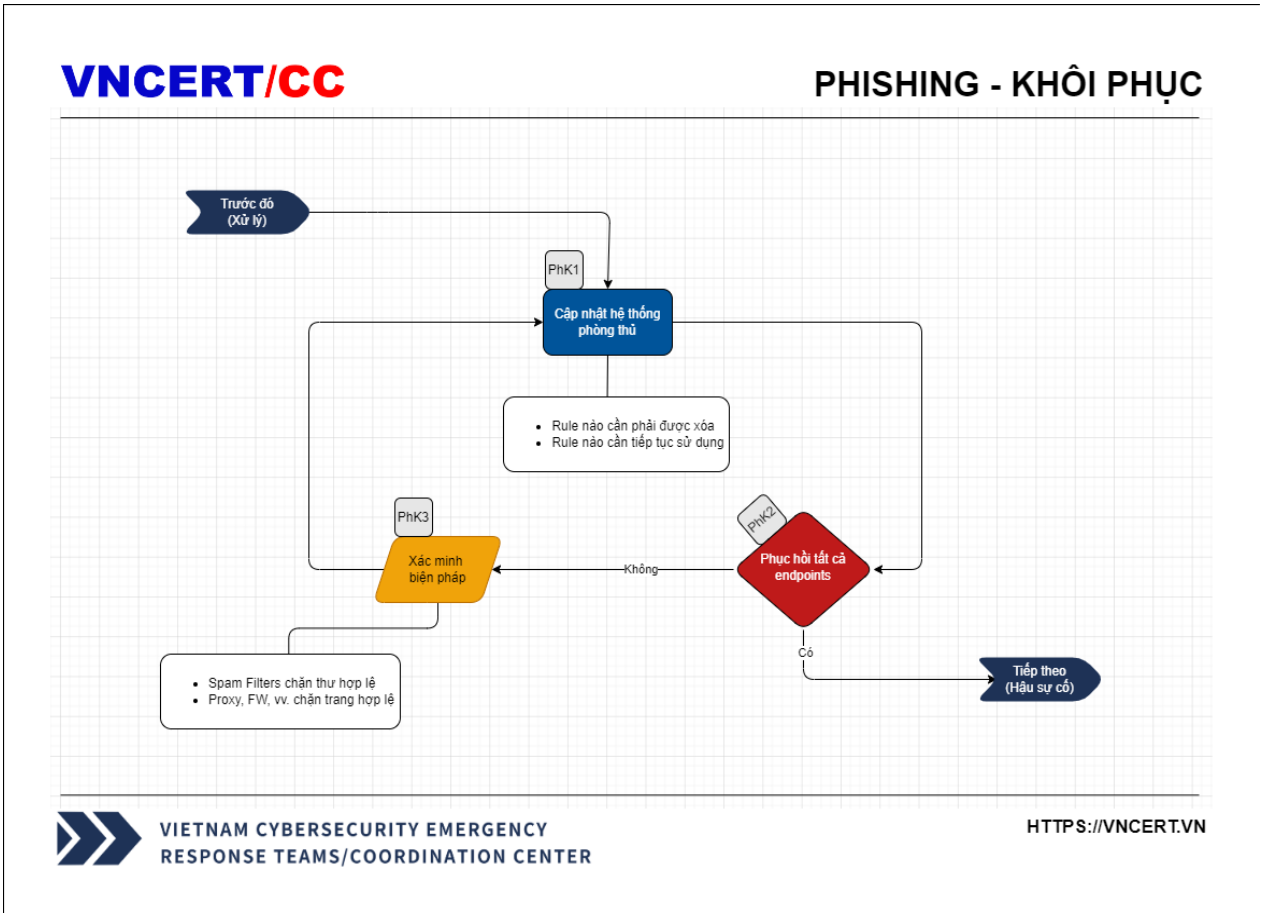
Nếu tất cả các endpoint bị ảnh hưởng đã được cách ly, ta có thể đi đến giai đoạn tiếp theo.

**Phát hiện IOC mới**

Nếu phát hiện được IOC mới, hãy quay lại Giai đoạn **Phân tích.**

## 2.6. Giai đoạn 5: Khôi phục

Giai đoạn này bao gồm các bước ngăn chặn và khắc phục, giảm thiểu ảnh hưởng của sự cố:




*Hình 5: Quy trình khôi phục*

### Cập nhật hệ thống phòng thủ

Xác định rule nào cần phải được xóa và cần phải tiếp tục sử dụng trong danh sách sau: Spam Filters, Firewall Rules, EDR (Ban hashes, Ban domains, cách ly), Proxy Block.

### Phục hồi tất cả endpoints

Nếu tất cả các endpoint bị ảnh hưởng đã được cách ly, ta có thể đi đến giai đoạn tiếp theo.

### Xác nhận các biện pháp đối phó

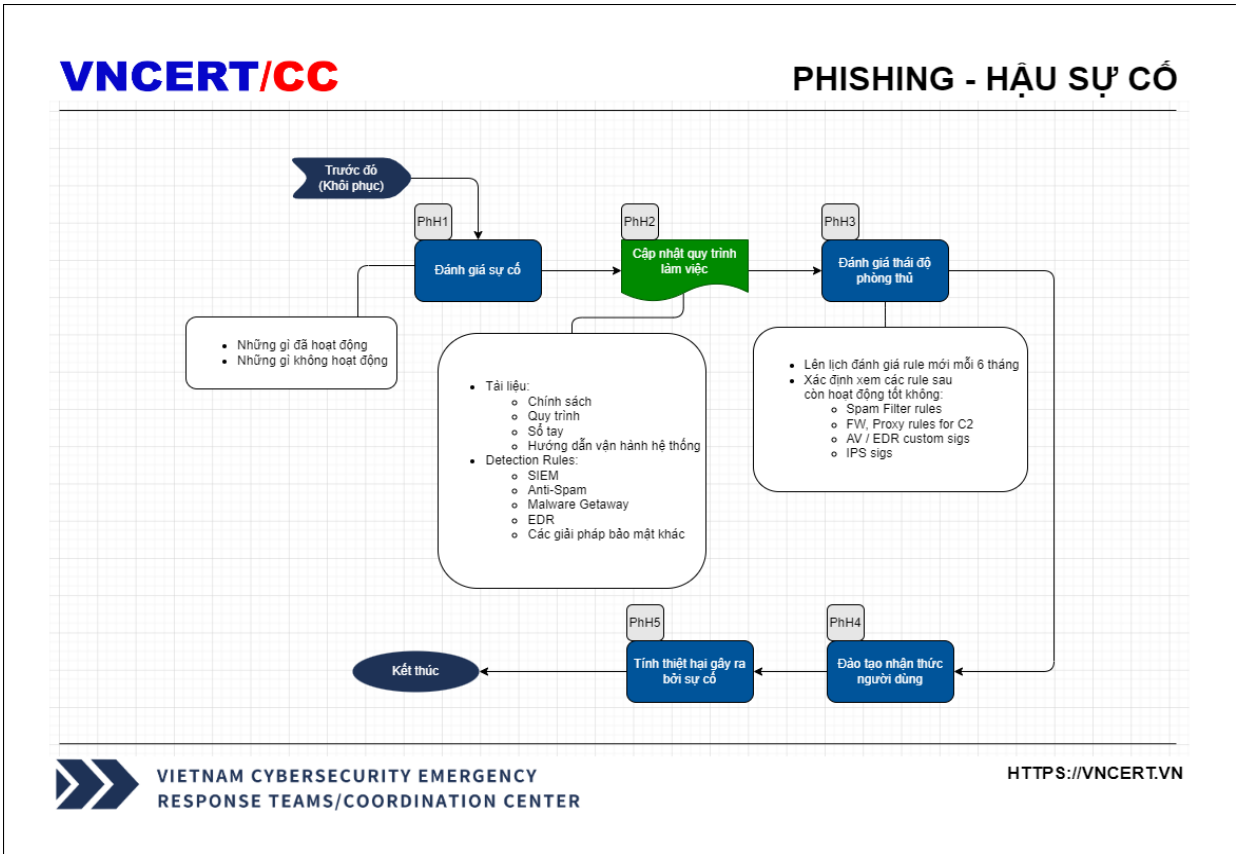
- Xác định xem các yêu cầu hợp lệ có bị chặn không: Spam Filters, Proxy, Firewall, EDR.

- Nếu có, hãy quay lại **Cập nhật hệ thống phòng thủ.**

- Nếu không thì đi đến giai đoạn tiếp theo.

### 2.7. Giai đoạn 6: Hậu sự cố

Giai đoạn này bao gồm các đánh giá cuối cùng về sự cố, cập nhật rule và hồ sơ:




*Hình 6: Quy trình hậu sự cố*

**Đánh giá sự cố**

- Những gì đã hoạt động.

- Những gì không hoạt động.

**Cập nhật quy trình làm việc**

- Cập nhật các tài liệu sau: chính sách, quy trình, sổ tay, hướng dẫn vận hành hệ thống.

- Cập nhật các rule trong: SIEM, Anti-Spam, Malware Getaway, EDR, các giải pháp bảo mật khác.

**Đánh giá thái độ phòng thủ**

- Lên lịch đánh giá rule mới mỗi 6 tháng

- Xác định xem các rule sau còn hoạt động: Spam Filter Rules, Firewall Rules, Proxy Rules, AV / EDR custom Signatures, IPS Signatures

**Đào tạo nhận thức của người dùng**

Đảm bảo rằng người dùng được nâng cao nhận thức về: cách nhận biết giả mạo, cách báo cáo giả mạo, nguy hiểm của các liên kết lạ, nguy hiểm của việc mở tập tin đính kèm.

**Đánh giá thiệt hại gây ra bởi sự cố**

Đánh giá các thiệt hại gây ra bởi sự cố dẫn đến:

- Chi phí bảo hiểm khi thông tin bi mật bị lộ.

- Chi phí khi kết nối không gian mạng không được bảo vệ hiệu quả khỏi phần mềm độc hại, tấn công, từ chối dịch vụ đi kèm hoặc sử dụng hay truy cập trái phép.

- Chi phí điều tra để xác định vị trí dễ bị hại, phân tích tác động, đảm bảo ngăn chặn và tính toán mức độ thiệt hại.

- Chi phí liên quan đến việc giải quyết các mối đe dọa tống tiền trong việc tiết lộ thông tin hoặc mã độc hại nếu các khoản tống tiền không được thanh toán.

### 3. Tài liệu tham khảo

Sổ tay này được xây dựng bằng cách sử dụng các tài liệu tham khảo sau:

https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=14tt1&1600804844570

https://www.gov.scot/publications/cyber-resilience-incident-management/

https://github.com/certsocietegenerale/IRM/tree/master/EN

https://www.incidentresponse.com/playbooks/

https://ayehu.com/cyber-security-incident-response-automation/top-5-cyber-security-incident-response-playbooks/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

**Thông tin liên hệ:** Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam **(VNCERT/CC)**

**Email:** ir@vncert.vn

**Số điện thoại:** 0869.100.317

**Địa chỉ:** Tầng 5, 115 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội