Sổ tay Ứng phó Sự cố Từ chối dịch vụ (DDoS)

Dự án: **Australian Government Cyber Security Training Development Program Vietnam - Chương trình Phát triển Năng lực An toàn thông tin của Chính phủ Úc dành cho Việt Nam**

Thụ hưởng: Mạng lưới ứng cứu sự cố an toàn không gian mạng quốc gia - Việt Nam

Tháng 1/2025

Nội dung

Danh mục các Bảng

Danh mục các Hình

1 Giới thiệu

1.1 Mục đích và mục tiêu

Sổ tay ứng phó sự cố từ chối dịch vụ (Distributed Denial of Service - DDoS Playbook) (gọi tắt là Sổ tay DDOS) này hỗ trợ cho các tổ chức thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (gọi tắt là Mạng lưới UCSC) xây dựng Kế hoạch Ứng cứu sự cố tấn công DDoS cụ thể.

Tài liệu này khuyến nghị các hành động nên thực hiện khi phát hiện Sự cố tấn công DDoS. Danh sách các hành động này có thể không đầy đủ, và các giai đoạn có thể được thực hiện đồng thời. Các tổ chức có thể bổ sung thêm các hành động ngoài các hướng dẫn trong Sổ tay này cũng như có thể giảm bớt các hành động được nêu trong Sổ tay nếu không phù hợp với quá trình ứng cứu sự cố thực tế.

Sổ tay này không bao gồm các hướng dẫn kỹ thuật cụ thể cho việc ứng phó.

Trong trường hợp xảy ra sự cố an toàn thông tin mạng nghiêm trọng, khuyến nghị các đơn vị tham khảo quy định tại Quyết định 05/2017/QĐ-TTg và báo cho cơ quan điều phối quốc gia hỗ trợ.

1.2 Đối tượng

Sổ tay DDoS này dành cho các đối tượng sau:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).
- Thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.
- Các tổ chức, doanh nghiệp trong nước có nhu cầu tham khảo, áp dụng.

1.3 Các tiêu chuẩn và khung tham chiếu

Các tiêu chuẩn và khung tham chiếu sau đã được xem xét trong quá trình phát triển Sổ tay này:

- Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ: **Hướng dẫn Xử lý Sự cố An ninh Máy tính, Hướng dẫn Xử lý Sự cố An ninh Máy tính (nist.gov)**, tham khảo chi tiết tại https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Trung tâm An ninh mạng Úc: **Hướng dẫn và Mẫu Kế hoạch Ứng cứu sự cố An ninh mạng, Kế hoạch Ứng cứu sự cố An ninh mạng, | Cyber.gov.au**, tham khảo chi tiết tại https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-incident-response-plan

Ngoài ra, Sổ tay DDoS này có tham khảo đến các cơ quan an toàn thông tin mạng của các quốc gia và các công ty an toàn thông tin mạng sau:

- Trung tâm An toàn mạng Úc ACSC (https://www.cyber.gov.au/)
- Trung tâm An toàn mạng Quốc gia Vương Quốc Anh (https://www.ncsc.gov.uk/)
- Cơ quan An toàn mạng và An toàn hạ tầng Hoa Kỳ (https://www.cisa.gov/)
- Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (https://www.nist.gov/)
- Cục An toàn thông tin (https://ais.gov.vn/)
- Viện Công nghệ SANS (https://www.sans.org/)
- CyberCX (https://cybercx.com.au/)

1.4 Ưu tiên ứng cứu sự cố

Các tổ chức Thành viên Mạng lưới UCSC sẽ ưu tiên tiến hành ứng cứu các sự cố an toàn thông tin mạng theo trình tự sau:

1) **Bảo vệ tính mạng và an toàn con người**: nếu một sự cố an toàn thông tin mạng có thể gây thương tích hoặc tử vong cho con người, ưu tiên hàng đầu trong việc ứng cứu với sự cố đó là bảo vệ an toàn của con người.
2) **Duy trì/khôi phục hoạt động của các hệ thống trọng yếu quốc gia**: nếu một sự cố an toàn thông tin mạng đang ảnh hưởng đến một hệ thống thông tin quan trọng cung cấp dịch vụ cho công dân Việt Nam, thì việc duy trì hoặc khôi phục hoạt động của hệ thống đó là ưu tiên.
3) **Thu thập bằng chứng kỹ thuật số**: nếu không xung đột với hai ưu tiên trên, việc thu thập bằng chứng thích hợp để hỗ trợ điều tra kỹ lưỡng về sự cố an toàn thông tin mạng và có thể đưa ra bằng chứng tại toà án là một ưu tiên.
4) **Phục hồi kịp thời sau sự cố**: nếu không xung đột với ba ưu tiên trên, ưu tiên sẽ là đảm bảo phục hồi nhanh chóng sau sự cố an toàn thông tin mạng và đưa hoạt động trở lại bình thường.

1.5 Thẩm quyền và Xem xét

[Giám đốc/Người được uỷ quyền của Tổ chức] có thẩm quyền phê duyệt tài liệu này để áp dụng trong toàn tổ chức.

Hàng năm, tài liệu này phải được *[Giám đốc/Người được uỷ quyền của Tổ chức]* xem xét để đảm bảo tài liệu luôn được cập nhật. Sử dụng Bảng 1 và Bảng 2 để ghi lại tất cả các cập nhật và phê duyệt đối với Sổ tay này.

Quản lý Tài liệu	
Tác giả	CyberCX – VNCERT/CC
Chủ sở hữu	Tổ chức …
Ngày tạo	
Tên người/đơn vị xem xét lần cuối	
Ngày xem xét lần cuối	
Tên người/đơn vị phê duyệt lần cuối và ngày	
Ngày xem xét tiếp theo	

Bảng 1: Quản lý và Xem xét Tài liệu

Phiên bản	Ngày phê duyệt	Được phê duyệt bởi	Mô tả thay đổi
1.0	…/…/2024	Cục An toàn thông tin	Bản hướng dẫn gửi thành viên Mạng lưới UCSC
1.1	…/…/2024		bản sửa đổi cho phù hợp với …

Bảng 2: Quản lý Phiên bản

2 Giới thiệu

DDoS là một loại tấn công mạng sử dụng mạng lưới các hệ thống bị xâm nhập để tràn ngập các trang web bằng các yêu cầu kết nối, khiến trang web hoặc máy chủ chậm lại và/hoặc không đáp ứng. Tấn công DDoS giới hạn khả năng sử dụng tài nguyên, ngăn người dùng hoạt động bình thường.

Tấn công DDoS có thể được phân loại là tấn công logic hoặc tấn công tràn ngập làm cạn kiệt tài nguyên.

- Tấn công logic lợi dụng các lỗ hổng bảo mật để khiến máy chủ hoặc dịch vụ bị ngừng hoặc chậm lại, làm giảm đáng kể hoạt động và hiệu suất bình thường.
- Tấn công tràn ngập làm cạn kiệt tài nguyên khiến tài nguyên của máy chủ hoặc mạng bị tiêu thụ quá mức, khiến nó không còn có thể phản hồi hoặc phản hồi bị giảm đáng kể.

Tấn công DDoS có thể xảy ra dưới dạng các cuộc tấn công độc lập. Tuy nhiên, các cuộc tấn công này cũng có thể được kết hợp với các mối đe dọa an toàn thông tin mạng khác, chẳng hạn như việc thực thi các phần mềm độc hại khác nhau.

Để đảm bảo ứng cứu sự cố hiệu quả đối với sự cố DDoS, các bước điều tra cần được thực hiện để liệt kê các sự kiện của sự cố, từ đó có thể thực hiện các bước ngăn chặn, loại bỏ và phục hồi tốt nhất. Khi thực hiện các bước điều tra, đội ứng cứu sự cố nên xem xét những điều sau:

- Quy mô và mức độ nghiêm trọng của sự cố.
- Phương thức xâm nhập.
- Tác động đến hoạt động, kinh doanh.

Trong suốt quá trình điều tra và loại bỏ, Đội ứng cứu sự cố nên điều chỉnh hành động của mình để loại bỏ hiệu quả mối đe dọa tương ứng với ba yếu tố trên.

2.1 Định nghĩa

Định nghĩa	Mô tả
Denial-of-service (DoS)	Một loại tấn công mà máy tính bị tấn công bởi một lượng lớn truy cập từ một hệ thống của hacker và làm quá tải hệ thống mục tiêu.
Distributed Denial-of-service (DDoS)	Một loại tấn công mà máy tính bị tấn công bằng lưu lượng truy cập từ nhiều hệ thống khác nhau thông qua nhiều địa điểm khác nhau.
Tấn công Volumetric	Làm quá tải và tràn ngập trang web, ứng dụng của nạn nhân với lưu lượng băng thông lớn cho đến khi hệ thống nạn nhân không thể xử lý lưu lượng. Các loại phổ biến bao gồm UDP Flood, ICMP flood, SYN flood, NTP Amplification, DNS Amplification
Tấn công Protocol	Tấn công Protocol, còn được gọi là tấn công làm cạn kiệt trạng thái, là do gián đoạn dịch vụ bằng cách tiêu thụ quá mức tài nguyên máy chủ và/hoặc tất cả tài nguyên trên thiết bị mạng. Các cuộc tấn công này thường nhắm mục tiêu vào các điểm yếu trong Lớp 3 và Lớp 4 của mô hình OSI. Các loại tấn công protocol phổ biến bao gồm Ping of Death và Smurf Attacks

Tấn công Application Layer	Tấn công lớp ứng dụng khai thác các lỗ hổng trong lớp ứng dụng gửi dữ liệu và các chức năng tới người dung (Lớp 7) bằng cách làm quá tải mục tiêu với số lượng yêu cầu hoặc giao dịch quá mức.

Bảng 3: Định nghĩa

3 Cách sử dụng Sổ tay

Sổ tay này mô tả chi tiết cách Đội ứng cứu sự cố sẽ phản ứng với các sự cố DDoS một cách hiệu quả.

Phần tài liệu	Mô tả
Giới thiệu và Tổng quan	
Phần 1-2	Trước khi bắt đầu quy trình ứng cứu sự cố DDoS, Sổ tay DDoS cung cấp phần giới thiệu nêu rõ mục đích, đối tượng, các tiêu chuẩn và khuôn khổ liên quan, các ưu tiên và bối cảnh. **Hướng dẫn sử dụng:** Đọc lần lượt các phần từ 1-2 để hiểu rõ quy trình chính của Sổ tay DDoS.
Điều tra	
Phần 4	Giai đoạn điều tra cung cấp cho đội ứng cứu sự cố các hành động cần được thực hiện khi ứng cứu với nhiều loại tấn công DDoS khác nhau. **Hướng dẫn sử dụng:** Đọc và làm theo các bước từ A1.01 đến A1.15 (đồng thời tham khảo các Phụ lục và Hình minh họa có liên quan). Các bước 'Quyết định' được sử dụng để tạm dừng quy trình để đưa ra quyết định trước khi quy trình có thể tiếp tục.
Ngăn chặn và Loại bỏ	
Phần 5	Giai đoạn ngăn chặn và loại bỏ nhằm mục đích hạn chế mức độ tác động của sự cố và sử dụng thông tin thu thập được từ giai đoạn điều tra để bảo vệ trước các cách thức tấn công và hạn chế sự di chuyển ngang (lateral movement). **Hướng dẫn sử dụng:** Đọc và làm theo các bước từ A2.01 đến A2.13 (đồng thời tham khảo các Phụ lục có liên quan). Các bước 'Quyết định' được sử dụng để tạo một khoảng dừng trong quy trình để đưa ra quyết định trước khi quy trình có thể tiếp tục.
Phục hồi	
Phần 6	Giai đoạn phục hồi nhằm mục đích xác định nguyên nhân của sự cố, thông báo các cải tiến trong tương lai hoặc triển khai các công nghệ kỹ thuật, cũng như xác nhận các bước khắc phục đã thực hiện trước đó và khôi phục mọi chức năng bị hạn chế. **Hướng dẫn sử dụng:** Đọc và làm theo các bước từ A3.01 đến A3.02 (đồng thời tham khảo các Phụ lục có liên quan).

Bảng 4: Cẩm nang sử dụng DDoS

4 Điều tra

Giai đoạn điều tra bao gồm đánh giá hoạt động mạng để xác định bản chất và quy mô của mối đe dọa. Quá trình này kết hợp việc thu thập bằng chứng, xác định các vectơ tấn công và đánh giá sơ bộ về tác động. Thông tin thu thập được trong giai đoạn này sẽ cung cấp thông tin về các bước khắc phục cần thiết để ngăn chặn và phục hồi thành công sau sự cố.

Xem chi tiết về quy trình điều tra trong bảng dưới đây.

<table>
<tr><th colspan="2">Hành động</th><th>Mô tả</th></tr>
<tr><td colspan="2">Điều tra Sự cố</td><td>Đội ứng cứu sự cố điều tra một sự cố DDoS.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>A1.01</td><td>Thu thập thêm thông tin</td><td>[Nhập chức danh liên quan]</td></tr>
<tr><td colspan="3">Mô tả hành động:</td></tr>
<tr><td colspan="3">Để thực hiện ứng cứu sự cố hiệu quả đối với một cuộc tấn công DDoS được báo, đội ứng cứu sự cố sẽ xem xét thông tin có sẵn, đảm bảo thấy và hiểu rõ các điểm sau:
• Kiến trúc mạng của hệ thống liên quan
• Loại tấn công đang được báo cáo
• Các bước giảm thiểu hiện tại đã thực hiện
Đội ứng cứu sự cố có thể nhận được báo cáo về các cuộc tấn công DDoS bị nghi ngờ, nhưng không có nghĩa đây là một cuộc tấn công mà có thể do nguyên nhân tải nặng (ví dụ: mức sử dụng cao) hoặc lỗi hệ thống không xác định. Khi thu thập thông tin thích hợp về sự cố được báo cáo, trước tiên cần xác định xem báo cáo đó là một cuộc tấn công hay một sự cố khác. Để làm như vậy, đội ứng cứu sự cố sẽ tìm cách trả lời các câu hỏi dưới đây:
• Hệ thống có đang chịu tải nặng chưa từng có trước đây không?
• Hệ thống trước đây đã có tiêu chuẩn / định mức khi hoạt động bình thường chưa?
➔ Nếu tải hệ thống bình thường, thì cần so sánh với lưu lượng quan sát được ở thời điểm hiện tại.
• Cuộc tấn công được báo cáo đối với một hệ thống cụ thể hay cuộc tấn công đang lan sang các hệ thống/ứng dụng khác?
• Người báo cáo có gặp bất kỳ hoạt động đáng ngờ nào khác trên hệ thống không?
• Người báo cáo có nhận được bất kỳ yêu cầu hoặc liên lạc nào liên quan đến DDoS được báo cáo không?
○ Nếu có, những yêu cầu hoặc liên lạc này là gì?
○ Chúng đến từ ai? Đó là một kẻ tấn công đã biết hay chưa biết?
○ Những yêu cầu pháp lý và quy định nào có thể cần được xem xét khi liên lạc với các tác nhân đe dọa tiềm ẩn?
• Cuộc tấn công được báo cáo xảy ra vào thời gian nào?
○ Thời gian đó có phản ánh thời gian gia tăng tải thông thường hay không?
• Có bất kỳ tình huống liên quan nào có thể giải thích việc tăng tải không, ví dụ như một sự kiện chính trị hoặc thể thao?</td></tr>
</table>

- Có bất kỳ sửa chữa hoặc gián đoạn dịch vụ nào đã biết có thể giải thích hoạt động bất thường không?
- Hệ thống bị ảnh hưởng có mất kết nối hoặc hoạt động với hiệu suất giảm không?

Sau khi hoàn thành, hãy chuyển đến bước 1.02.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.02	Điều tra Nhật ký/Ứng dụng	[Nhập chức danh liên quan]

Mô tả hành động::

[Nhập chi tiết kỹ thuật về nhật ký ứng dụng/điều tra]

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.03	Xem xét các tài sản quan trọng quốc gia	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố sẽ xem xét các tài sản quan trọng của quốc gia bị ảnh hưởng. Nếu có, theo bất kỳ cách nào bởi cuộc tấn công này, cần liên lạc với chủ sở hữu tài sản có liên quan ngay lập tức.

Sau khi hoàn thành, hãy chuyển đến bước A1.04.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.04	Xác định loại tấn công	[Nhập chức danh liên quan]

Đội ứng cứu sự cố nên xem xét và cân nhắc loại tấn công. ~~Các cuộc~~ Tấn công DDoS thường rơi vào ba loại (tuy nhiên, chúng có thể kết hợp nhiều hơn từ các loại này và có thể sử dụng các chiến thuật khác nhau):

Tấn công dựa trên khối lượng (Volume-Based attacks): Làm quá tải và tràn ngập trang web nạn nhân với lưu lượng băng thông lớn cho đến khi hệ thống nạn nhân không thể xử lý lưu lượng. Tấn công này sẽ được đo bằng bit, megabit hoặc gigabit trên giây trên băng thông gửi đến hệ thống nạn nhân.

Tấn công Protocol: loại tấn công tạo ra các giao thức để nhắm mục tiêu vào các biện pháp mà các trang web sử dụng để tự bảo vệ như tường lửa. Các cuộc tấn công giao thức cố gắng vô hiệu hóa các biện pháp bảo vệ này, cho phép chúng tấn công các lỗ hổng. Tấn công này có thể được đo bằng số lượng gói tin được gửi đến hệ thống nạn nhân, số gói tin mỗi giây pps (packets per second)

Tấn công tầng ứng dụng: loại tấn công nhắm mục tiêu cụ thể vào các ứng dụng cụ thể cung cấp nội dung và chức năng chính cho người dùng. Đo lường cuộc tấn công này bằng cách kiểm tra số lượng yêu cầu (RPS – request per second) được gửi đến máy chủ.

Tấn công DDoS sử dụng các chiến lược và kiểu xâm phạm khác: sử dụng kết hợp nhiều chiến lược để đạt được tác động tối đa. Ứng cứu sự cố sẽ điều tra loại tấn công và xem xét điều này trong suốt giai đoạn ngăn chặn và xóa bỏ.

Sau khi hoàn thành, hãy chuyển đến bước A1.05.

#	Nhiệm vụ	Người chịu trách nhiệm:

A1.05	Xem xét các khía cạnh mục tiêu và mục tiêu tấn công DDoS	[Nhập chức danh liên quan]

Mô tả hành động:

Để ngăn chặn, loại bỏ và phục hồi thành công sau DDoS, đội ứng cứu sự cố sẽ cần hiểu các chiến thuật mà kẻ tấn công đã hoặc đang sử dụng để phá hoại (các) khu vực dịch vụ, hệ thống và mạng của tổ chức nạn nhân.

Tuân theo các hướng dẫn về an toàn thông tin mạng được khuyến nghị, đội ứng cứu sự cố sẽ xem xét và điều tra tác động đối với:

- Kết nối mạng.
- Tính toán.
- Lưu trữ

Tham khảo Phụ lục A để biết các cân nhắc về điều tra DDoS.

Sau khi hoàn thành, hãy tiếp tục bước A1.06.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.06	Điều tra tác động của cuộc tấn công	[Nhập chức danh liên quan]

Mô tả hành động:

Sau khi xác định loại tấn công (Bước A1.03) và mục tiêu cũng như chiến thuật của cuộc tấn công (Bước A1.04), đội ứng cứu sự cố sẽ thực hiện các bước điều tra thêm để hiểu tác động của cuộc tấn công.

Đội ứng cứu sự cố sẽ phải trả lời các câu hỏi dưới đây:

- Các tài sản đã bị gián đoạn trong bao lâu?
- Cuộc tấn công đang diễn ra hay không còn?
- Những bên liên quan nào đã bị ảnh hưởng? Chẳng hạn như:
    - Nhân viên
    - Khách hàng
    - Đối tác chuỗi cung ứng
    - Công chúng
- Có những tác động rộng hơn cần được xem xét ngoài dịch vụ hoặc mạng bị ảnh hưởng không?
- Có bao nhiêu dịch vụ không khả dụng hoặc bị chậm?
- Tấn công này ảnh hưởng tới một bộ phận hay toàn bộ tổ chức?
- Các hệ thống công cộng bị ảnh hưởng có hiển thị thông báo lỗi hay không?
- Các địa chỉ IP có đang gửi một số lượng các yêu cầu kết nối bất thường không?
- Hậu quả của việc mất kết nối trong thời gian dài là gì?

- Đây có phải là lần đầu mạng hoặc hệ thống bị tấn công hay không?

Ngoài ra, đội ứng cứu sự cố sẽ sử dụng bất kỳ hệ thống phát hiện tấn công mạng sẵn có, cũng như yêu cầu thông tin các bên liên quan bị ảnh hưởng.

Sau khi hoàn thành, hãy tiếp tục bước A1.07.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.07	Phân loại tác động của cuộc tấn công	[Nhập chức danh liên quan]

Mô tả hành động:

Sau các bước điều tra trên, đội ứng cứu sự cố sẽ xác định mức độ nghiêm trọng hiện tại của sự cố và phân loại sự cố thành một trong các mức dưới đây:

- **Từ chối dịch vụ hoàn toàn:**
  - Dịch vụ bị ảnh hưởng không thể hoạt động theo mọi cách, ngăn hoạt động, kinh doanh bình thường.
- **Từ chối dịch vụ vừa phải:**
  - Dịch vụ bị ảnh hưởng chậm hoặc không liên tục.
  - Có thể duy trì hoạt động kinh doanh.
- **Từ chối dịch vụ tối thiểu**, dẫn đến dịch vụ chậm hoặc bị đình trệ.
  - Dịch vụ bị chậm không liên tục.
  - Tác động đến hoạt động kinh doanh hạn chế hoặc không tác động.

Những tình trạng trên cần cho việc thiết lập các sự kiện được thống nhất chung trong nhóm ứng phó sự cố và cho mục đích báo cáo. Lưu ý những tuyên bố này cần phải được xem xét thường xuyên.

Phân loại bản chất của cuộc tấn công, cùng với việc truyền đạt rõ ràng về mức độ nghiêm trọng của cuộc tấn công, sẽ giúp các cấp cao bên trong và bên ngoài của các bên liên quan hiểu được mức nghiêm trọng của sự cố.

Sau khi hoàn tất, hãy tiến hành 'Quyết định: Phương thức liên lạc chính có bị ảnh hưởng hay bị nghi ngờ bị ảnh hưởng bởi sự cố DDoS không?'.

Sau khi hoàn thành, hãy chuyển đến bước A1.08.

Quyết định: Phương thức liên lạc chính có bị ảnh hưởng hoặc bị nghi ngờ là bị ảnh hưởng bởi sự cố DDoS hay không?	• Nếu có – Tiếp tục bước 1.08. • Nếu không – Tiếp tục bước 1.09.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.08	Thiết lập kênh liên lạc riêng	[Nhập chức danh liên quan]

Mô tả hành động:

Nếu thích hợp, đội ứng cứu sự cố sẽ xem xét chuyển sang kênh liên lạc riêng nếu DDoS đã ảnh hưởng đến khả năng liên lạc nội bộ. Kênh liên lạc riêng là cách thức liên lạc khác kênh liên lạc chính. Ngoài ra, kênh liên lạc riêng có thể cần thiết khi có dự đoán rằng kẻ tấn công đã có quyền truy cập hoặc kiểm soát kênh liên lạc chính.

Hãy xem xét những điều sau khi quyết định xem có cần kênh liên lạc riêng hay không:

- Liệu có nghi ngờ rằng cuộc tấn công đã ảnh hưởng đến các kênh liên lạc nội bộ hay không.

- Liệu có nghi ngờ rằng kẻ tấn công đã xâm phạm hoặc truy cập các kênh liên lạc chính hay không?

Sau khi xem xét các cân nhắc trên, đội ứng cứu sự cố sẽ thiết lập một kênh liên lạc riêng nếu cần.

Sau khi hoàn thành, hãy tiếp tục bước A1.09.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.09	Phân tích mạng	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố sẽ tìm cách điều tra nguồn gốc của cuộc tấn công DDoS. Nếu có thể, việc kiểm tra dịch vụ và hệ thống bị ảnh hưởng nên được thực hiện để xác định xem sự cố lan rộng hay cục bộ đối với thiết bị đầu cuối của người dùng.

Việc giám sát hoạt động mạng phải tiếp tục trong suốt quá trình ứng cứu sự cố, vì kẻ tấn công sẽ tiếp tục thay đổi cách thức để tìm kiếm các ứng dụng hoặc giao thức web dễ bị tấn công.

Sau khi hoàn thành, hãy tiếp tục bước A1.10.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.10	Xác định và điều tra IP	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố cần kiểm tra kỹ các công cụ và nhật ký giám sát mạng để xác định phạm vi IP đang được sử dụng để phát động tấn công DDoS và duy trì cập nhật danh sách các địa chỉ IP độc hại. Điều tra IP cũng nên mở rộng các việc thăm dò IP độc hại, trinh sát, các dấu hiệu xâm nhập IOC (Indicators of Compromise) và các nỗ lực tấn công mật khẩu kiểu vét cạn.

Danh sách các vấn đề này sẽ là hướng dẫn thực hiện các nỗ lực loại bỏ quan trọng, sẽ giải thích kỹ hơn ở phần sau của tài liệu.

Tham khảo Phụ lục B để biết thêm thông tin về Điều tra IP.

Sau khi hoàn thành, hãy tiếp tục bước A1.11.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.11	Xác định động cơ của kẻ tấn công	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố tìm hiểu động cơ của kẻ tấn công, có thể bao gồm một hoặc nhiều điều sau đây:

- Lợi ích kinh tế
- Hủy hoại danh tiếng
- Chính trị
- Hành động quân sự
- Theo chủ nghĩa hack (Hacktivism) cổ súy cho những quan điểm cá nhân

Sau khi hoàn thành, hãy tiếp tục bước A1.12.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.12	Điều tra các Lỗ hổng Bảo mật Phổ	[Nhập chức danh liên quan]

	biến (CVE) tiềm ẩn được sử dụng trong cuộc tấn công	

Mô tả hành động:

Nếu có thể, đội ứng cứu sự cố sẽ xem xét tất cả thông tin thu thập được trong giai đoạn điều tra và xác định xem liệu trong cuộc tấn công ransomware có khai thác CVE mới hay CVE đã có hay không.

Xem bảng dưới đây để biết các tài nguyên CVE được đề xuất:

Nguồn CVE chính thức	URL
NIST	https://nvd.nist.gov/
MITRE	https://cve.mitre.org/
Trung tâm An toàn mạng quốc gia Vương quốc Anh	https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

Bảng 5 : Các nguồn CVE

Các nguồn thông tin bổ sung	URL
Offensive Security, danh bạ khai thác dành cho kiểm những người thử, nghiên cứu và hack đạo đức	https://www.exploit-db.com/
Trung tâm An toàn mạng quốc gia Úc	https://www.cyber.gov.au/acsc/view-all-content/advisories
Danh bạ lỗ hổng của VulDB	https://vuldb.com/
Nguồn tra cứu CVE ưa thích của đội ứng cứu sự cố	[Nhập công cụ CVE ưa thích của đội ứng cứu sự cố]

Bảng 6: Các nguồn thông tin Bổ sung

Sau khi hoàn thành, hãy tiếp tục bước A1.13

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.13	Xác định các yêu cầu hỗ trợ từ bên thứ ba	[Nhập chức danh liên quan]

Mô tả hành động:

Nếu đội ứng cứu sự cố xác định một vụ DDoS lớn , cần cân nhắc xem xét lại nhà cung cấp bên thứ ba. Các sự cố DDoS quy mô lớn có thể cần triển khai các công nghệ giảm thiểu DDoS chuyên dụng.

Để điều tra nhu cầu chưa rõ đối với các biện pháp giảm thiểu như vậy, đội ứng cứu sự cố nên trả lời các câu hỏi sau:

- Ước tính chi phí của sự cố là bao nhiêu, nếu sự cố tiếp tục với tốc độ hiện tại?
- Chi phí này so với chi phí hỗ trợ giảm thiểu DDoS từ bên thứ ba như thế nào?

Sau khi hoàn thành, hãy tiếp tục bước A1.14.

#	Nhiệm vụ	Người chịu trách nhiệm:
A1.14	Xem xét việc phân loại lại	[Nhập chức danh liên quan]
Mô tả hành động:		
Sau các bước trên, đội ứng cứu sự cố nên xem xét liệu cuộc điều tra có phát hiện bằng chứng về sự xâm nhập thêm hay không, kể cả phần mềm độc hại. Việc phát hiện thêm sự xâm nhập có thể thay đổi loại sự cố và có thể cần thông báo cho lãnh đạo các bên liên quan. Đồng thời các bước tiếp theo trong sổ tay này sẽ hỗ trợ giảm thiểu các tác động tiếp theo của sự cố DDoS, việc xác định thêm sự xâm nhập có thể yêu cầu cập nhật và phân loại lại sự cố nếu thích hợp. Sau khi hoàn thành, hãy tiếp tục bước A1.15.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A1.15	Liên hệ với Nhà cung cấp Bảo hiểm	[Nhập chức danh liên quan]
Mô tả hành động:		
Nếu có thể, đội ứng cứu sự cố sẽ làm việc với tổ chức bị ảnh hưởng để liên hệ với nhà cung cấp bảo hiểm nếu có để thảo luận về các lựa chọn bảo hiểm tiềm tàng cho sự cố DDoS. Đội ứng cứu sự cố và tổ chức bị ảnh hưởng sẽ điều tra: • Chính sách bảo hiểm mạng bao gồm những gì? • Có bất kỳ trường hợp loại trừ nào sẽ áp dụng cho sự cố DDoS không? Sau khi hoàn thành, hãy tiếp tục bước A1.16.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A1.16	Cập nhật Thẻ (ticket) Sự cố	[Nhập chức danh liên quan]
Mô tả hành động:		
Cập nhật thẻ sự cố với tất cả thông tin thu thập được trong suốt giai đoạn điều tra này. Sau khi hoàn thành, hãy tiếp tục đến phần Ngăn chặn và Loại bỏ.		

Bảng 7: Quy trình điều tra

5 Ngăn chặn và Loại bỏ

Ngăn chặn và loại bỏ sự cố DDoS là quá trình thực hiện kiểm soát mạng, hỗ trợ từ bên thứ ba và các nỗ lực khắc phục khác để hạn chế tác động của cuộc tấn công. Ngăn chặn chủ yếu tập trung vào việc bảo mật để các kiểu tấn công không thể khai thác thêm, trong khi các nỗ lực loại bỏ tập trung vào việc giảm thiểu hoàn toàn cuộc tấn công và cho phép hoạt động hàng ngày trở lại bình thường.

Lưu ý: Sự trưởng thành và kiến trúc của mạng và/hoặc hệ thống bị ảnh hưởng sẽ có nhiều thay đổi và ảnh hưởng đối với việc ban hành các biện pháp giảm thiểu DDoS hiệu quả. Các biện pháp giảm thiểu DDoS hiệu quả nhất phải được thử nghiệm và triển khai trước khi xảy ra tấn công.

Xem chi tiết về giai đoạn ngăn chặn và loại bỏ trong phần dưới đây.

<table>
<tr><th colspan="2">Hành động</th><th>Mô tả</th></tr>
<tr><td colspan="2">Ngăn chặn Sự cố</td><td>Đội ứng cứu sự cố ngăn chặn sự cố DDoS.</td></tr>
<tr><td>#</td><td>Nhiệm vụ</td><td>Người chịu trách nhiệm:</td></tr>
<tr><td>A2.01</td><td>Phát triển và triển khai chiến lược ngăn chặn</td><td>[Nhập chức danh liên quan]</td></tr>
<tr><td colspan="3">Mô tả hành động:</td></tr>
<tr><td colspan="3">Phát triển và triển khai chiến lược ngăn chặn cho sự cố DDoS. Cân nhắc những điều sau đây khi phát triển chiến lược thực hiện:
Yêu cầu bảo quản bằng chứng;
Tính khả dụng của dịch vụ (ví dụ: kết nối mạng, dịch vụ được cung cấp cho các bên bên ngoài);
Thời gian và tài nguyên cần thiết để thực hiện chiến lược;
Hiệu quả của chiến lược (ví dụ: ngăn chặn một phần, ngăn chặn toàn bộ);
Thời gian của giải pháp để ngăn chặn toàn bộ (ví dụ: yêu cầu ứng cứu sự cố trong vòng 48 giờ, giải pháp thường trực);
Lập kế hoạch phê duyệt các biện pháp ngăn chặn có khả năng gây gián đoạn để giảm thiểu thiệt hại.
Sau khi hoàn thành, hãy tiếp tục bước A2.02.</td></tr>
<tr><td>#</td><td>Nhiệm vụ</td><td>Người chịu trách nhiệm:</td></tr>
<tr><td>A2.02</td><td>Liên hệ với các bên liên quan</td><td>[Nhập chức danh liên quan]</td></tr>
<tr><td colspan="3">Mô tả hành động:</td></tr>
<tr><td colspan="3">Trong trường hợp các dịch vụ không khả dụng do cuộc tấn công DDoS, đội ứng cứu sự cố xem xét thông báo cho nhân viên có liên quan để giảm thiểu sự gián đoạn và lây lan.
Xem Phụ lục C về mẫu thông báo được đề xuất.
Lưu ý: Trong trường hợp giả mạo hoặc mạo danh tên miền/trang web hàng loạt, đội ứng cứu sự cố có thể cần xem xét sự cần thiết của hỗ trợ từ bên thứ ba.
Sau khi hoàn thành, hãy tiếp tục bước A2.03</td></tr>
</table>

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.03	Thông báo gián đoạn dịch vụ	[Nhập chức danh liên quan]
Mô tả hành động:		
Trong trường hợp các dịch vụ trực tuyến đang bị gián đoạn, đội ứng cứu sự cố sẽ liên hệ với đơn vị bị ảnh hưởng để đặt thông báo trên trang web của tài sản hoặc dịch vụ bị ảnh hưởng. Tùy thuộc vào mức độ nghiêm trọng của dịch vụ bị đang bị gián đoạn, thông báo cho người dùng về sự gián đoạn dịch vụ có thể giúp giảm thiểu nguy cơ phản ứng mạnh từ công chúng/truyền thông. Tham khảo Phụ lục D để tham khảo các mẫu truyền thông. Sau khi hoàn thành, hãy tiếp tục bước A2.04.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A2.04	Cân nhắc hỗ trợ từ cloud hoặc CDN	[Nhập chức danh liên quan]
Mô tả hành động:		
Nếu có thể, đội ứng cứu sự cố có thể tạm thời chuyển các dịch vụ trực tuyến sang lưu trữ trên cloud bởi một nhà cung cấp dịch vụ cloud có băng thông cao và mạng phân phối nội dung CDN có thể cache các trang web non-dynamic. Bước này có thể hỗ trợ duy trì hoạt động của dịch vụ đồng thời có thể chịu tải lớn hơn. Nếu đang sử dụng CDN, hãy tránh tiết lộ địa chỉ IP của máy chủ web gốc và cân nhắc sử dụng tường lửa để đảm bảo rằng chỉ CDN mới có thể truy cập máy chủ web này. Sau khi hoàn thành, hãy tiếp tục bước A2.05.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A2.05	Xem xét và cấu hình lại các tường lửa	[Nhập chức danh liên quan]
Mô tả hành động:		
Đội ứng cứu sự cố sẽ xem xét việc liên hệ với quản trị tường lửa của mạng bị ảnh hưởng. Nên cân nhắc những điều sau: • Cách cải thiện quy tắc tường lửa (dựa trên thông tin tình báo thu thập được trong giai đoạn điều tra). • Xem xét việc cấu hình tường lửa và bộ định tuyến để chặn các địa chỉ /dãi IP trái phép và đóng các cổng không cần thiết. Sau khi hoàn thành, hãy tiếp tục bước A2.06		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A2.06	Liên hệ với ISP để chặn hoặc chuyển hướng lưu lượng	[Nhập chức danh liên quan]
Mô tả hành động:		

Đội ứng cứu sự cố sẽ xem xét việc liên hệ với các Nhà cung cấp dịch vụ Internet (ISP) có liên quan để yêu cầu chặn lưu lượng truy cập có chọn lọc, tùy thuộc vào bản chất của tấn công.

- Nếu có một số ít kẻ tấn công thay đổi địa chỉ IP không thường xuyên:
  - Từ chối truy cập một cách chọn lọc vào các địa chỉ IP tham gia vào cuộc tấn công DDoS.
- Nếu có một số lượng lớn (hàng trăm, đến hàng nghìn) kẻ tấn công:
  - Xem xét thực hiện chiến lược chặn theo địa lý, các địa chỉ IP bên ngoài Việt Nam được chuyển hướng và từ chối truy cập.
  - Cân nhắc thay đổi địa chỉ IP của máy chủ đang bị nhắm mục tiêu hoặc thay đổi cả tên miền DNS và địa chỉ IP.

Sau khi hoàn thành, hãy tiếp tục bước A2.07.

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.07	Bảo tồn tài nguyên	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố sẽ xác định những dịch vụ nào có thể tạm thời tắt để bảo tồn băng thông nhằm duy trì tính khả dụng cho các dịch vụ quan trọng hoặc dễ bị tổn thương nhất của tổ chức/mạng. Nếu thực hiện như vậy, xem xét các câu hỏi dưới đây:

- Các cổng nào đang bị nhắm mục tiêu? Có thể chặn chúng không?
- Các cổng nào có thể được giới hạn tốc độ để giới hạn số lượng gói tin tối đa được truyền mỗi giây?
- Những dịch vụ nào không quan trọng và có thể tạm thời tắt?
- Những dịch vụ nào quan trọng nhất đối với các hoạt động đang diễn ra của tổ chức/mạng bị nhắm mục tiêu?

Ngoài ra, đội ứng cứu sự cố nên tắt bất kỳ chức năng nào hoặc xóa nội dung khỏi các dịch vụ trực tuyến đang cho phép cuộc tấn công DDoS có hiệu quả, đảm bảo ghi nhật ký các thay đổi để có thể khôi phục dịch vụ. Một số hành động có thể thực hiện gồm:

- Triển khai phiên bản trang web nào sử dụng tài nguyên thấp (nếu có)
- Loại bỏ chức năng tìm kiếm
- Loại bỏ nội dung động hoặc các tệp lớn

Sau khi hoàn thành, hãy tiếp tục bước A2.08.

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.08	Triển khai dịch vụ giảm thiểu	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố nên cân nhắc việc triển khai dịch vụ giảm thiểu DDoS trong thời gian diễn ra tấn công. Đội ứng cứu sự cố sẽ xem xét các câu hỏi bên dưới trước khi lựa chọn nhà cung cấp dịch vụ giảm thiểu:

- Nhà cung cấp dịch vụ có tự động áp dụng các biện pháp giảm thiểu DoS không? Họ có thông báo cho đơn vị bị ảnh hưởng khi làm như vậy không?

- Nhà cung cấp dịch vụ có điều chỉnh băng thông vượt quá giới hạn nhất định không?
- Mất bao lâu để bật các biện pháp giảm thiểu bổ sung? Làm thế nào để làm điều này?
- Đơn vị bị ảnh hưởng có bị tính phí cho việc sử dụng tài nguyên vượt mức không?
- Nhà cung cấp có quyền chấm dứt dịch vụ của đơn vị bị ảnh hưởng hoặc 'đưa lưu lượng truy cập vào sink hole' để tránh ảnh hưởng đến các khách hàng khác của nhà cung cấp dịch vụ không? (máy chủ DNS sinkhole dùng để phát hiện và chặn tất cả các lưu lượng độc hại, có thể cả các lưu lượng truy cập khác)
- Nhà cung cấp dịch vụ có liên hệ trước khi hành động không?
- Dịch vụ của đơn vị bị ảnh hưởng có thể được kích hoạt lại nhanh chóng như thế nào nếu bị tắt?

Sau khi hoàn thành, hãy tiếp tục bước A2.09.

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.09	Xây dựng chiến lược loại bỏ	[Nhập chức danh liên quan]

Mô tả hành động:

Xây dựng chiến lược loại bỏ dựa trên thông tin thu thập được và việc ưu tiên tài sản, được thiết lập trong giai đoạn ngăn chặn và điều tra. Cân nhắc những điều sau đây:

- Làm thế nào để chống lại cuộc tấn công?
- Những bên liên quan nào trong nội bộ hoặc bên ngoài có thể cần tham gia để loại bỏ sự cố? Chẳng hạn như:
    - Các nhà cung cấp bên thứ ba
    - Các nhà cung cấp dịch vụ kết nối
    - Các lĩnh vực kinh doanh/chính phủ cụ thể có quyền kiểm soát hoặc quyền hạn đối với một số tài sản nhất định
- Nếu có thể áp dụng, quy trình nào có thể được cải thiện dựa trên những bài học kinh nghiệm từ các sự cố trước đó?

Sau khi hoàn thành, hãy tiếp tục bước A2.10.

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.10	Tăng băng thông	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố sẽ xem xét tăng băng thông của hệ thống bị ảnh hưởng để giảm tác động của sự cố.

Lưu ý: Bước này có thể chỉ hỗ trợ tạm thời và không nên dựa vào nó như một giải pháp.

Sau khi hoàn thành, hãy chuyển đến 'Quyết định: Sự cố có liên quan đến 'email bombing' hay email spam hàng loạt hay không?'

Quyết định:	
Sự cố có liên quan đến 'email bombing' hay email spam hàng loạt hay không?	• Nếu có – Tiếp tục bước A2.11 • Nếu không – Tiếp tục bước A2.12

#	Nhiệm vụ	Người chịu trách nhiệm:

A2.11	Giảm thiểu thư rác	[Nhập chức danh liên quan]

Mô tả hành động:

Một số hoạt động có thể thực hiện để giảm thiểu tác động của thư rác mà đội ứng cứu sự cố nên xem xét:

- 'Tarpitting' để chặn hoặc làm chậm lưu lượng truy cập từ một hoặc nhiều IP. (tarpitting email hoạt động bằng việc trì hoãn phản hồi cho một email đến, thường bằng cách thêm độ trễ giữa mỗi phản hồi SMTP từ máy chủ thư, khiến phần mềm của kẻ tấn công phải chờ phản hồi lâu hơn, làm chậm khả năng gửi thêm thư rác của chúng).
- Thiết lập các quy tắc email để lọc thư rác.
  - Điều chỉnh các quy tắc tùy thuộc vào các từ phổ biến được sử dụng trong email spam.
- Giảm hoặc giới hạn kích thước tệp đính kèm email tối đa.
- Chặn các tệp đính kèm email phổ biến trong các cuộc tấn công bom email, (ví dụ: các loại tệp .rar, .exe và .zip).
- Giảm hoặc tắt phản hồi tự động đối với email.

Lưu ý: Đội ứng cứu sự cố không nên xóa hàng loạt email. Sau khi hoàn thành, hãy tiếp tục bước A2.12

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.12	Lọc địa chỉ MAC	[Nhập chức danh liên quan]

Mô tả hành động:

Tùy thuộc vào bản chất của tấn công DDoS, đội ứng cứu sự cố nên xem xét cải thiện việc giới hạn hoặc xác thực địa chỉ MAC. Việc thay đổi, chỉnh sửa hoặc giới hạn địa chỉ MAC có thể cung cấp một giải pháp thay thế ngắn hạn trong cuộc tấn công DDoS. Việc thay đổi địa chỉ này có thể ngăn kẻ tấn công nhắm mục tiêu vào một số máy chủ nhất định. Tuy nhiên, các kẻ tấn công có thể giả mạo địa chỉ MAC và nhắm mục tiêu lại các máy chủ.

Đội ứng cứu sự cố sẽ đánh giá mức độ của cuộc tấn công, liên hệ với ISP có liên quan và cân nhắc thực hiện các biện pháp ngắn hạn này nếu thích hợp.

Sau khi hoàn thành, hãy tiếp tục bước A2.13.

#	Nhiệm vụ	Người chịu trách nhiệm:
A2.13	Cân nhắc triển khai một blackhole	[Nhập chức danh liên quan]

Mô tả hành động:

Đội ứng cứu sự cố sẽ xem xét việc cố gắng đưa lưu lượng mạng vào blackhole để giảm tải cho hệ thống bị ảnh hưởng.
(trong kỹ thuật blackhole, lưu lượng mạng đến địa chỉ IP mục tiêu được chuyển hướng đến một 'blackhole' là một khoảng trống ảo loại bỏ tất cả lưu lượng đến mà không chuyển đến người nhận dự định. Khi xảy ra một cuộc tấn công DDoS, người quản trị có thể chuyển hướng tất cả lưu lượng vào địa chỉ IP mục tiêu đến một blackhole đã thiết lập sẵn).

Lưu ý: Đội ứng cứu sự cố cần xem xét biện pháp này có thể ảnh hưởng như thế nào đến lưu lượng hợp pháp. Có thể các địa chỉ IP biến đổi đang được sử dụng, điều này giới hạn hiệu quả của bước này.

Sau khi hoàn thành, hãy tiếp tục đến phần Phục hồi.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A2.14	Di chuyển ứng dụng	[Nhập chức danh liên quan]
Mô tả hành động::		
[Nhập chi tiết kỹ thuật về chuyển ứng dụng sang nơi khác (Application Migration)]		

Bảng 8: Quy trình Ngăn chặn và Loại bỏ

6 Phục hồi

Giai đoạn phục hồi nhằm phục hồi và khôi phục từ sự cố, đồng thời xác định các nguyên nhân để cải tiến trong tương lai.

Xem bảng dưới đây để biết chi tiết về các bước liên quan đến phục hồi.

Hành động		**Mô tả**
Phục hồi Sự cố		Đội ứng cứu sự cố khôi phục sau sự cố DDoS.
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A3.01	Xác thực việc loại bỏ và khôi phục chức năng	[Nhập chức danh liên quan]
Mô tả hành động:		
Khôi phục môi trường về trạng thái hoạt động bình thường. Việc khôi phục này bao gồm: • Cấu hình mạng trở lại chức năng bình thường • Khôi phục dữ liệu từ các bản sao lưu, nếu cần thiết • Xây dựng lại các điểm cuối bị xâm nhập • Khôi phục các điểm cuối bị xâm nhập từ các bản sao lưu sạch (nếu có thể) để loại bỏ các thay đổi đối với tài sản thông tin • Loại bỏ sự cô lập cho các hệ thống đã được làm sạch trong giai đoạn loại bỏ • Xem xét và loại bỏ bất kỳ quy tắc tường lửa tạm thời và thay đổi cấu hình tạm thời nào cần thiết cho các giai đoạn ngăn chặn và loại bỏ trước đó Sau khi hoàn thành, hãy tiếp tục bước A3.02		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A3.02	Phục hồi	[Nhập chức danh liên quan]
Mô tả hành động:		
Sau giai đoạn loại bỏ, Đội ứng cứu sự cố sẽ tiếp tục phần Phục hồi trong Kế hoạch ứng cứu sự cố an toàn thông tin mạng CSIRP. Ngoài ra, đội ứng cứu sự cố cũng sẽ tham khảo phần Cập nhật cho cấp Điều hành và phần Xem xét Bài học Kinh nghiệm của CSIRP.		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A3.03	Phục hồi ứng dụng	[Nhập chức danh liên quan]
Mô tả hành động::		
[Nhập chi tiết kỹ thuật về phục hồi ứng dụng]		
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
A3.04	Sau sự cố	[Nhập chức danh liên quan]
Mô tả hành động:		

Sau khi phục hồi, đội ứng cứu sự cố cũng sẽ tham khảo phần Cập nhật cho cấp Điều hành và phần Xem xét Bài học Kinh nghiệm của Kế hoạch ứng cứu sự cố CSIRP.

Bảng 9: Quy trình Khôi phục

Phụ lục A: Xác định Hệ thống Mục tiêu

Ứng cứu sự cố hiệu quả chống lại nhiều loại tấn công DDoS khác nhau đòi hỏi sự hiểu biết sâu sắc về các hệ thống bị tấn công nhắm mục tiêu. Các cuộc tấn công DDoS thường nhắm mục tiêu vào nhiều điểm trong dịch vụ, mạng và hệ thống của một tổ chức, các điểm này có thể ngăn chặn hoặc làm giảm việc cung cấp các dịch vụ thiết yếu. Cần hiểu rõ về các điểm này để cho phép đội ứng cứu sự cố thực hiện các biện pháp giảm thiểu cần thiết.

Tuân theo các thực tiễn tốt nhất trong ngành về an toàn thông tin mạng, đội ứng cứu sự cố sẽ xem xét và điều tra tác động đối với:

- Kết nối mạng
- Tính toán
- Lưu trữ
- Tác động ở cấp độ hệ thống
- Dữ liệu

Đội cũng cần xem xét và đánh giá tác động của cuộc tấn công DDoS đối với:

- Danh tiếng
- Người dùng
- Nền kinh tế

Kết nối mạng

Kết nối mạng của nạn nhân là liên kết giữa dịch vụ của họ và người dùng hoặc các thành phần trong dịch vụ. Khi điều tra và tìm hiểu về kết nối mạng, hãy xem xét:

Khía cạnh cần xem xét	Mô tả
Các dịch vụ/mạng được đặt cùng vị trí	Tùy thuộc vào cấu hình, một số mạng/hệ thống có thể được đặt cùng vị trí trên một liên kết mạng cũng được sử dụng bởi các dịch vụ khác. Các dịch vụ này có thể dễ bị gián đoạn, vì có khả năng một cuộc tấn công tinh vi lợi dụng cấu hình để tác động đến cả hai dịch vụ được kết nối. Ví dụ: nếu hai bộ hoặc ngành sử dụng một dịch vụ được đặt cùng vị trí, thì tác động DDoS đối với bên này cũng có thể tác động đến bên kia.
Kết nối bên ngoài	Nếu mạng và/hoặc dịch vụ được người dùng truy cập qua internet, thì dịch vụ sẽ có dung lượng được cung cấp bởi nhà cung cấp dịch vụ internet. Tùy thuộc vào sự tinh vi của kẻ tấn công và bản chất của cuộc tấn công, bất kỳ sự gia tăng nào về dung lượng đều có thể làm giảm tác động tải hoặc cho phép cuộc tấn công bão hòa băng thông mới được cung cấp.
Giao diện quản lý	Nếu mạng được quản lý bởi các giao diện quản lý do nạn nhân kiểm soát, thì kẻ tấn công có thể nhắm mục tiêu vào các giao diện này và ngăn

	chặn hoạt động của dịch vụ trong một cuộc tấn công.
Dung lượng mạng nội bộ	Giống như mạng bên ngoài, mạng nội bộ có dung lượng hữu hạn có thể được tăng hoặc giảm. Dung lượng này có thể góp phần vào tác động của sự cố.

Bảng 10: Các khía cạnh kết nối mạng cần xem xét

Tính toán

Sức mạnh tính toán và/hoặc tài nguyên tính toán có sẵn để phục vụ các yêu cầu dịch vụ và/hoặc dịch vụ là một thành phần quan trọng có thể bị nhắm mục tiêu bởi DDoS. Thông thường, điều này có thể trông giống như sự gia tăng đột biến của các yêu cầu sử dụng nhiều tài nguyên máy tính, dẫn đến việc làm chậm dịch vụ mục tiêu. Khi điều tra và tìm hiểu về sức mạnh tính toán, hãy xem xét:

Khía cạnh cần xem xét	Mô tả
Dung lượng ứng dụng	Dung lượng ứng dụng mạng và/hoặc dịch vụ có thể là mục tiêu cho DDoS. Khía cạnh tính toán này có thể bị quá tải.
Dung lượng cơ sở dữ liệu	Cơ sở dữ liệu có dung lượng và sức mạnh khác nhau để thực hiện các truy vấn và hành động tốn kém về mặt tính toán. Nếu một hệ thống dễ bị tổn thương bởi các truy vấn sử dụng nhiều tài nguyên, thì dung lượng truy vấn cơ sở dữ liệu có thể bị nhắm mục tiêu.
Lỗi dây chuyền	Tùy thuộc vào kiến trúc của mạng và/hoặc dịch vụ, một cuộc tấn công vào phía dịch vụ có thể dẫn đến lỗi trên các dịch vụ sử dụng chung tài nguyên, chẳng hạn như giao diện người dùng của một máy chủ web được kết nối.

Bảng 11: Các khía cạnh tính toán cần xem xét

Lưu trữ

Các mạng và dịch vụ có các mức lưu trữ khác nhau có thể bị ảnh hưởng hoặc nhắm mục tiêu trong một sự cố DDoS. Khi điều tra và tìm hiểu về bộ nhớ của nạn nhân, hãy xem xét:

Khía cạnh cần xem xét	Mô tả
Nhật ký ứng dụng	Nhật ký ứng dụng được sử dụng để xử lý các hành động, ghi dữ liệu vào nhật ký có liên quan. Việc lưu trữ này có thể bị nhắm mục tiêu thông qua DDoS bằng cách lặp đi lặp lại một hành động ghi một số lượng lớn nhật ký, cuối cùng làm quá tải dung lượng.
Bộ nhớ máy chủ cục bộ (lưu trữ và/hoặc truyền tệp)	Tùy thuộc vào mục đích của dịch vụ, bộ nhớ dịch vụ cục bộ có thể chịu trách nhiệm nhận các tệp và lưu trữ chúng. Khía cạnh này có thể bị

	nhắm mục tiêu thông qua việc tải lên/truyền hàng loạt các tệp để làm quá tải dung lượng.

Bảng 12: Các khía cạnh lưu trữ cần xem xét

Tất cả các khía cạnh trên nên được điều tra để hiểu rõ hơn về cách thức tấn công DDoS nhắm mục tiêu vào nạn nhân và tác động mà nó gây ra.

Phụ lục B: Điều tra địa chỉ IP

Tùy thuộc vào sự tinh vi của cuộc tấn công, có thể xác định được các địa chỉ IP được sử dụng để phát động tấn công. Đội ứng cứu sự cố nên ghi chú những chi tiết này, vì các bước trong giai đoạn ngăn chặn sẽ yêu cầu thông tin này.

Việc sử dụng hàng loạt bot, kết hợp với giả mạo IP quy mô lớn là một chiến thuật phổ biến trong các cuộc tấn công tinh vi. Thông thường, điều này đạt được thông qua việc làm giả nội dung trong tiêu đề IP bằng các số ngẫu nhiên để che giấu IP người gửi (hoặc để khởi động cuộc tấn công DDoS kiểu phản xạ).

Trong trường hợp tấn công botnet, giả mạo IP có thể được sử dụng trên các thiết bị máy chủ bị xâm nhập để tránh bị phát hiện, ngăn chặn thông báo về các máy chủ bị xâm nhập và bỏ qua các tập lệnh bảo mật cố gắng đưa vào danh sách đen các địa chỉ IP tấn công. Đội ứng cứu sự cố nên cố gắng theo dõi những kẻ tấn công này, nắm bắt:

- Địa chỉ IP.
- Vị trí địa lý
- Nhà cung cấp mạng
- Tình trạng hệ thống
- Sử dụng tài nguyên:
    - Sử dụng RAM
    - Sử dụng CPU
    - Sử dụng GPU
    - Sử dụng đĩa
- Lưu lượng băng thông mạng
- Tốc độ truy cập
- Kết nối TCP/IP hiện tại
- Số lượng gói tin theo loại (SYN/ACK/RST)

Đội cũng nên thực hiện quét trước khi tấn công và thăm dò và kiểm tra khai thác như một phần của việc này.

Lưu ý:

- Các kẻ tấn công có thể nhanh chóng thay đổi cơ sở hạ tầng, cho phép họ tránh các biện pháp chặn trong một số trường hợp.
- Trong trường hợp tấn công botnet tinh vi với khối lượng lớn, việc theo dõi tất cả các địa chỉ IP vi phạm có thể không thực tế hoặc hiệu quả.

Phụ lục C: Mẫu Thông báo cho Nhân viên

Mẫu Thông báo cho Nhân viên
Từ: [Đơn vị] Đến: [Nhập các bên liên quan] Chủ đề: KHẨN CẤP: [Nhập dòng chủ đề liên quan] Chào buổi sáng/chiều/tối [Nhập chức danh/tên người nhận], [Nhập tên] đang liên hệ với bạn để thông báo về một cuộc tấn công từ chối dịch vụ (DDoS) chống lại [Nhập tài sản]. Một cuộc tấn công DDoS vô hiệu hóa hoặc từ chối truy cập vào các dịch vụ hướng ra internet bằng cách làm quá tải nó với các yêu cầu thông tin giả, tiêu thụ tất cả băng thông khả dụng và ngăn người dùng hợp pháp truy cập dịch vụ. Sự cố được khai báo là [Nhập tóm tắt sự cố, bao gồm các dịch vụ bị ảnh hưởng bởi cuộc tấn công DDoS]. Đội ứng cứu sự cố đang [Nhập các hành động hiện tại]. Nếu bạn biết về các dịch vụ bổ sung bị ảnh hưởng bởi cuộc tấn công DDoS này mà không được xác định ở trên, vui lòng thông báo cho [Nhập chi tiết liên hệ]. [Bao gồm bất kỳ hướng dẫn nào liên quan đến việc tương tác với giới truyền thông, cách tiếp tục công việc và bất kỳ cân nhắc nào khác] Chúng tôi đánh giá cao sự hợp tác của bạn. Trân trọng, [Nhập chức danh hoặc tên]

Hình 1: Mẫu Thông báo cho Nhân viên

Phụ lục D: Truyền thông về gián đoạn dịch vụ

Trong trường hợp gián đoạn dịch vụ, đội ứng cứu sự cố sẽ làm việc để thông báo với người dùng nhằm hạn chế phản ứng tiêu cực từ công chúng/truyền thông.

Nhắn tin rõ ràng và liên tục là một bước cực kỳ quan trọng trong việc duy trì danh tiếng của đơn vị bị ảnh hưởng.

Xem các banner được đề xuất dưới đây có thể được hiển thị trên phiên bản tĩnh của dịch vụ web bị ảnh hưởng:

Tùy chọn 1	Tùy chọn 2	Tùy chọn 3
"Chúng tôi biết rằng một số khách hàng đang gặp sự cố với [dịch vụ/hệ thống] và chúng tôi đang khẩn trương điều tra nguyên nhân của những sự cố này. Chúng tôi cảm ơn bạn đã kiên nhẫn và xin lỗi vì bất kỳ sự bất tiện nào gây ra."	"Chúng tôi biết rằng một số khách hàng đang gặp sự cố với [dịch vụ/hệ thống] và chúng tôi đang khẩn trương điều tra nguyên nhân của những sự cố này. Chúng tôi cảm ơn bạn đã kiên nhẫn và sẽ cung cấp thông tin cập nhật về tình hình trong thời gian sớm nhất."	"Một sự cố an toàn thông tin mạng đang ảnh hưởng đến [danh sách các dịch vụ bị ảnh hưởng]. Chúng tôi đang nỗ lực để khôi phục các dịch vụ này nhanh chóng và an toàn nhất có thể. Chúng tôi xin lỗi vì sự gián đoạn và cảm ơn sự kiên nhẫn của bạn. Các cập nhật và thông tin chi tiết khác có thể được tìm thấy ở đây: [Liên kết liên quan]"

Bảng 13: Các banner để hiển thị trên trang web bị ảnh hưởng

Các banner trên được thiết kế để nằm ở đầu trang web bị ảnh hưởng.

Trong trường hợp phản ứng tiêu cực từ công chúng và/hoặc truyền thông có thể gây ra hậu quả nghiêm trọng về tài chính, danh tiếng và/hoặc pháp lý, khuyến nghị Đội ứng cứu sự cố làm việc với tổ chức bị ảnh hưởng hoặc cơ quan nhà nước để thực hiện một số hoạt động truyền thông sau đây:

Phương thức	Mục đích
Thông báo qua email/tin nhắn văn bản cho khách hàng/người dùng	Phương thức giao tiếp này sẽ tiếp cận một lượng lớn đối tượng và cho phép đơn vị bị ảnh hưởng kiểm soát thông tin.
Đăng trên các trang mạng xã hội có liên quan	"Ngoài việc tiếp cận khách hàng của mình, một bài đăng trên mạng xã hội cũng sẽ tiếp cận đối tượng bên ngoài khách hàng, cho phép hiển thị thêm các bước chủ động đang được thực hiện để đối phó với sự cố an toàn thông tin mạng độc hại."
Cập nhật thông tin liên tục trên tất cả các kênh truyền thông	Giao tiếp liên tục trên tất cả các kênh truyền thông cung cấp phủ sóng rộng.

Bảng 14: Các phương thức truyền thông bổ sung

KẾT THÚC TÀI LIỆU