Mã độc

Chương 9. Phát hiện và xử lý sự cố mã độc

Mục tiêu

- Giới thiệu quy trình xử lý sự cố mã độc

Tài liệu tham khảo

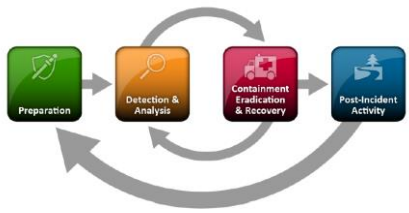
[1] TS. Lương Thế Dũng, KS. Hoàng Thanh Nam, 2013, Giáo trình Mã độc, Học viện kỹ thuật Mật mã

[2] NIST.SP.800-61r2

Nội dung

Nội dung

Quy trình xử lý sự cố mã độc



Incident Response Life Cycle

Chuẩn bị

Giai đoạn ban đầu của phản ứng sự cố phần mềm độc hại bao gồm thực hiện các hoạt động chuẩn bị:

- ❑ Phát triển các quy trình xử lý sự cố dành riêng cho phần mềm độc hại
- ❑ Chương trình đào tạo cho các đội ứng phó sự cố
- ❑ Xây dựng bộ công cụ

7

Phát hiện và phân tích

- ❑ Cảnh báo cho tổ chức bắt cứ khi nào sự cố xảy ra
- ❑ Phát hiện sớm các sự cố phần mềm độc hại

8

Ngăn chặn, loại bỏ và hồi phục

- ❑ Giảm thiểu tác động của phần mềm độc hại
- ❑ Tiêu diệt các tác hại của mã độc
- ❑ Phục hồi sau sự cố

9

Hoạt động sau sự cố

- ❑ Báo cáo chi tiết nguyên nhân và thiệt hại
- ❑ Các bước cần thực hiện để ngăn ngừa sự cố trong tương lai
- ❑ Chuẩn bị hiệu quả để xử lý các sự cố sẽ xảy ra trong tương lai

10

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

11

Chuẩn bị

Các tổ chức nên thực hiện các biện pháp chuẩn bị để đảm bảo rằng họ có khả năng ứng phó hiệu quả với các sự cố phần mềm độc hại:

- ❑ Chuẩn bị xử lý sự cố
- ❑ Ngăn ngừa sự cố

12

Chuẩn bị xử lý sự cố

Tài nguyên dùng để phân tích sự cố:

- ❑ **Tài liệu**
- ❑ **Sơ đồ mạng và danh sách các tài sản quan trọng**
- ❑ **Đường cơ sở hiện tại của mạng, hệ thống và hoạt động ứng dụng dự kiến**
- ❑ **Giá trị hàm băm mật mã của các tập tin quan trọng**

13

Ngăn ngừa sự cố

- ❑ **Đánh giá rủi ro định kỳ của các hệ thống và ứng dụng**
- ❑ **Ngăn chặn phần mềm độc hại: Phần mềm phát hiện và ngăn chặn phần mềm độc hại**
- ❑ **Nhận thức và đào tạo người dùng**

14

Nội dung

1. **Quy trình xử lý sự cố mã độc**
2. **Chuẩn bị**
3. **Phát hiện và phân tích**
4. **Ngăn chặn**
5. **Loại bỏ**
6. **Phục hồi**
7. **Các hoạt đông sau sự cố**

15

Phát hiện và phân tích

- ❑ **Dấu hiệu của sự cố**
- ❑ **Phân tích sự cố**
- ❑ **Tài liệu hóa sự cố, thông báo sự cố**

16

Dấu hiệu của sự cố

Sự cố có thể được phát hiện thông qua nhiều phương tiện khác nhau: Khả năng phát hiện tự động bao gồm IDPS, dựa trên mạng và máy chủ lưu trữ, phần mềm chống vi-rút và máy phân tích nhật ký; vấn đề được báo cáo bởi người dùng.

17

Source	Description
	Alerts
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.[1]
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.

18

Phân tích sự cố

Các khuyến nghị để làm cho phân tích sự cố dễ dàng và hiệu quả hơn:

- ❑ Hồ sơ mạng và hệ thống
- ❑ Hiểu các hành vi bình thường
- ❑ Tạo Chính sách lưu giữ nhật ký
- ❑ Thực hiện tương quan sự kiện
- ❑ Giữ đồng bộ tất cả máy chủ
- ❑ Thu thập dữ liệu bổ sung, lọc dữ liệu
- ❑ Sử dụng công cụ tìm kiếm Internet để nghiên cứu

19

Tài liệu hóa sự cố, thông báo sự cố

Các yếu tố liên quan đến sự cố:

- ❑Tác động chức năng của sự cố
- ❑Tác động thông tin của sự cố
- ❑Khả năng phục hồi từ sự cố

Thông báo sự cố: CIO, Trưởng phòng an ninh thông tin, nhân viên an ninh thông tin

20

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

21

Ngăn chặn

- ❑ Chọn chiến lược ngăn chặn
- ❑ Thu thập và xử lý bằng chứng
- ❑ Xác định máy chủ tấn công

22

Chọn chiến lược ngăn chặn

Tiêu chí để xác định chiến lược phù hợp:

- ❑ Thiệt hại tiềm tàng và trộm cắp tài nguyên
- ❑ Cần bảo quản bằng chứng
- ❑ Tính khả dụng của dịch vụ (ví dụ: kết nối mạng, dịch vụ được cung cấp cho bên ngoài)

23

Chọn chiến lược ngăn chặn

Tiêu chí để xác định chiến lược phù hợp:

- ❑ Thời gian và nguồn lực cần thiết để thực hiện chiến lược
- ❑ Hiệu quả của chiến lược (ví dụ: ngăn chặn một phần, ngăn chặn hoàn toàn)
- ❑ Thời gian

24

Thu thập và xử lý bằng chứng

Một bản ghi chi tiết nên được lưu giữ cho tất cả các bằng chứng:

- ❑ Xác định thông tin (vị trí, số sê-ri, số kiểu máy, tên máy chủ, địa chỉ MAC và địa chỉ IP của máy tính)
- ❑ Tên, tiêu đề và số điện thoại của từng cá nhân đã thu thập hoặc xử lý bằng chứng trong quá trình điều tra
- ❑ Thời gian của mỗi lần xử lý bằng chứng
- ❑ Vị trí lưu trữ chứng cứ

25

Xác định máy chủ tấn công

Các hoạt động được thực hiện phổ biến nhất để tấn công nhận dạng máy chủ:

- ❑ Xác thực địa chỉ IP tấn công máy chủ tấn công
- ❑ Nghiên cứu máy chủ tấn công thông qua công cụ tìm kiếm
- ❑ Sử dụng cơ sở dữ liệu sự cố
- ❑ Giám sát các kênh truyền thông của kẻ tấn công có thể

26

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

27

Loại bỏ

- ❑ Mục tiêu chính của là loại bỏ phần mềm độc hại khỏi các máy chủ bị nhiễm.
- ❑ Các tình huống khác nhau đòi hỏi sự kết hợp khác nhau của các kỹ thuật, các công cụ phổ biến nhất để diệt trừ: phần mềm phòng chống mã độc, công nghệ quản lý lỗ hổng, phần mềm kiểm soát truy cập mạng…

28

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

29

Phục hồi

Phục hồi có thể bằng các hành động như:

- ❑ Khôi phục hệ thống từ bản sao lưu sạch,
- ❑ Xây dựng lại hệ thống từ đầu,
- ❑ Thay thế các tập tin bị xâm nhập bằng các phiên bản sạch,
- ❑ Cài đặt các bản vá, thay đổi mật khẩu
- ❑ Thắt chặt an ninh mạng vành đai

30

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

31

Các hoạt đông sau sự cố

Sau một sự cố liên quan đến mã độc các đơn vị tổ chức cần thực hiện những công việc:

❑ Sửa đổi chính sách an ninh, chính sách bảo mật có thể ngăn ngừa sự cố tương tự,

❑ Đào tạo nâng cao nhận thức bảo mật cho người sử dụng,

32

Các hoạt đông sau sự cố

❑ Cấu hình lại các phần mềm, hệ điều hành hoặc cấu hình ứng dụng để hỗ trợ chính sách bảo mật,

❑ Triển khai, cấu hình lại phần mềm phát hiện mã độc.

33

Nội dung

1. Quy trình xử lý sự cố mã độc
2. Chuẩn bị
3. Phát hiện và phân tích
4. Ngăn chặn
5. Loại bỏ
6. Phục hồi
7. Các hoạt đông sau sự cố

34

Kapersky rescure disk