Họ tên: _____ Ngày: _____ Điểm: _____

Phân tích phần mềm độc hại và giảm thiểu mối đe dọa Hướng dẫn

Trojan, ransomware, phần mềm gián điệp, rootkit, sandbox ảo hóa, cách ly

TỔNG QUAN HỌC TẬP VỀ PHÂN TÍCH PHẦN MỀM ĐỘC HẠI

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về phân tích và phòng ngừa phần mềm độc hại. Bạn sẽ khám phá phần mềm gián điệp, trojan, tải trọng ransomware, công cụ dịch ngược, hành vi của rootkit và các chiến lược ngăn chặn lây lan.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- [ ] **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- [ ] **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- [ ] **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- [ ] **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- [ ] **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/phan-mem-doc-hai/

Lộ trình học về giảm thiểu phần mềm độc hại của bạn

- Phân biệt các loại phần mềm độc hại Trojan, sâu máy tính và rootkit.
- Triển khai thực thi ảo hóa sandbox để phân tích mã.
- Thiết kế kế hoạch ngăn chặn và làm sạch đối với các tải trọng ransomware đang hoạt động.

HƯỚNG DẪN PHÂN TÍCH PHẦN MỀM ĐỘC HẠI

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về việc giảm thiểu phần mềm độc hại. Kết thúc với hoạt động thưởng Nghĩ nhanh.

PHÂN TÍCH PHẦN MỀM ĐỘC HẠI VÀ NGĂN CHẶN MỐI ĐE DỌA (GIỚI THIỆU)

Mã độc như Trojan, sâu máy tính và ransomware gây ra các mối đe dọa có tác động lớn đối với thiết bị đầu cuối và máy chủ. Các nhóm bảo mật phân tích phần mềm độc hại trong hộp cát ảo và thực hiện nhanh các biện pháp cô lập mạng để ngăn tải trọng lan rộng.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Đặc điểm nhận dạng của ngựa Trojan (Trojan horse) là gì?**
   - A. Giả dạng phần mềm hợp pháp để lừa người dùng chạy nó
   - B. Tự sao chép qua các đường mạng nội bộ
   - C. Nó lây nhiễm vào các tệp bên trong môi trường ảo cô lập (sandbox)
   - D. Nó chặn bắt lưu lượng của nhà cung cấp dịch vụ internet

2. **2. Loại phần mềm độc hại nào mã hóa tệp và đòi thanh toán?**
   - A. Ransomware
   - B. Phần mềm gián điệp
   - C. Rootkit
   - D. Phần mềm quảng cáo

3. **3. Điều gì đại diện cho phần mềm gián điệp?**
   - A. Phần mềm độc hại được thiết kế để bí mật theo dõi thao tác gõ phím và hoạt động trình duyệt của người dùng
   - B. Mã chương trình chạy bên trong một container ảo cô lập
   - C. Bản cập nhật chống phần mềm độc hại tải từ các registry cơ sở dữ liệu
   - D. Tự động điều chỉnh độ sáng màn hình

4. **4. Vì sao các nhà phát triển phần mềm độc hại dùng rootkit?**
   - A. Để che giấu các tiến trình đang chạy và tệp độc hại khỏi hệ điều hành
   - B. Tăng tốc độ xử lý của CPU trên thiết bị đầu cuối
   - C. Để sao lưu tệp cơ sở dữ liệu vào kho đám mây an toàn
   - D. Để cải thiện thời lượng pin trên máy tính xách tay

5. **5. Sandboxing nghĩa là gì trong phân tích phần mềm độc hại?**
   - A. Thực thi các tệp đáng ngờ trong một hầm ảo biệt lập để quan sát hành vi một cách an toàn
   - B. Quét mã băm tệp so với cơ sở dữ liệu mối đe dọa đã biết
   - C. Khôi phục bản sao lưu cơ sở dữ liệu sau một vụ xâm nhập
   - D. Ngắt router mạng cục bộ khỏi đường truyền công cộng

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Sâu máy tính cần người dùng tương tác để lây lan qua các mạng cục bộ.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Adware luôn vô hại và không theo dõi hành vi người dùng hay lịch sử trình duyệt.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Khôi phục các bản sao lưu ngoại tuyến sạch cho phép nạn nhân lấy lại các tệp bị mã hóa mà không phải trả tiền chuộc.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Phần mềm diệt virus dựa trên chữ ký luôn ngăn chặn đáng tin cậy phần mềm độc hại zero-day trước khi có bất kỳ chữ ký nào cho nó.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Phần mềm độc hại không dùng tệp thực thi các tập lệnh độc hại trong bộ nhớ hệ thống, tránh ghi tệp vào ổ đĩa.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Phần mềm độc hại ngụy trang thành chương trình tiện ích an toàn là một _____ .
2. Các tải trọng độc hại khóa hệ thống cơ sở dữ liệu để đòi tiền được gọi là _____ .
3. Keylogger lặng lẽ ghi lại mật khẩu là một dạng _____ .
4. Ẩn sâu trong nhân của hệ điều hành cần có một _____ .
5. Phân tích các tệp đáng ngờ trong một kho cách ly là dùng một _____ ảo.
6. Ngăn chặn sự lây lan của các tải trọng phần mềm độc hại đang hoạt động đòi hỏi phải _____ mạng ngay lập tức.

NGÂN HÀNG TỪ VỰNG

CÔ LẬP · KHÔNG TỆP · MÃ ĐỘC TỐNG TIỀN · PHẦN MỀM GIÁN ĐIỆP · ROOTKIT · SANDBOX · SÂU MÁY TÍNH · TROJAN

Viết câu trả lời của bạn tại đây:

1.
2.
3.
4.
5.
6.

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

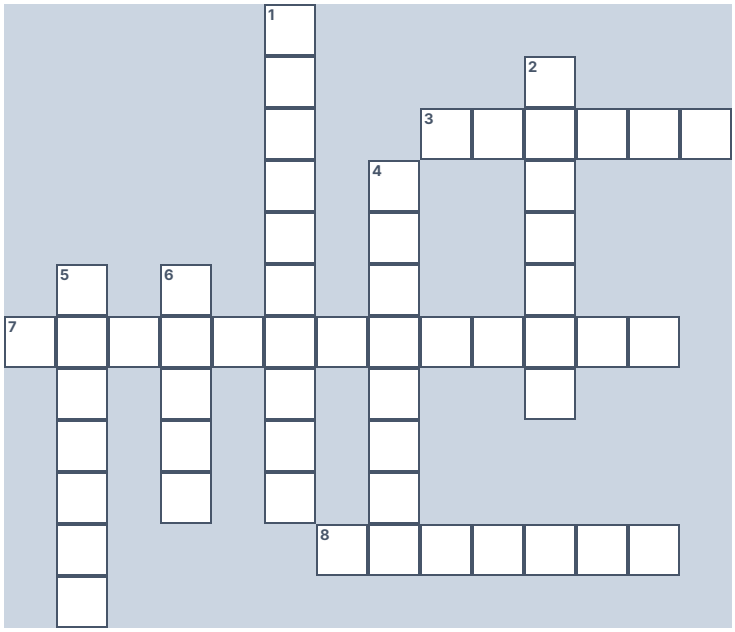
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. TROJAN	A	Chương trình được thiết kế để bí mật theo dõi và ghi lại hoạt động và dữ liệu nhập của người dùng.
☐	2. RANSOMWARE	B	Phần mềm độc hại chạy trực tiếp trong RAM để tránh bị trình quét đĩa phát hiện.
☐	3. PHẦN MỀM GIÁN ĐIỆP	C	Hạn chế các điểm cuối bị nhiễm để ngăn lây lan mã độc đe dọa.
☐	4. ROOTKIT	D	Phần mềm độc hại ngụy trang thành một tiện ích vô hại hoặc hữu ích.
☐	5. SANDBOX	E	Phần mềm độc hại tự nhân bản lây lan qua các mạng mà không cần hành động của con người.
☐	6. NGĂN CHẶN	F	Phần mềm độc hại mã hóa bộ nhớ hệ thống và đòi thanh toán để giao khóa.
☐	7. SÂU MÁY TÍNH	G	Môi trường ảo cô lập dùng để phân tích tệp độc hại một cách an toàn.
☐	8. KHÔNG DÙNG TỆP	H	Phần mềm độc hại ẩn mình sâu trong nhân hệ thống để duy trì quyền kiểm soát quản trị.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

3. Phần mềm độc hại ngụy trang thành một chương trình tiện ích vô hại hoặc hữu ích (6)

7. Phần mềm độc hại mã hóa bộ nhớ hệ thống và đòi tiền để giao khóa giải mã (13)

8. Chương trình được thiết kế để bí mật theo dõi và ghi lại hoạt động và thông tin nhập của người dùng (7)

HÀNG DỌC

1. Phần mềm độc hại tự nhân bản, lây lan qua mạng mà không cần con người thao tác (10)

2. Phần mềm độc hại ẩn sâu trong nhân hệ thống để duy trì quyền quản trị (7)

4. Phần mềm độc hại thực thi trực tiếp trong RAM để tránh bị trình quét ổ đĩa phát hiện (8)

5. Môi trường ảo tách biệt dùng để phân tích tệp độc hại một cách an toàn (7)

6. Hạn chế các thiết bị đầu cuối bị nhiễm để ngăn các tải trọng đe dọa lây lan (5)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

3 hàng ngang: Phần mềm độc hại ngụy trang thành một chương trình tiện ích vô hại hoặc hữu ích (6 chữ cái):

7 hàng ngang: Phần mềm độc hại mã hóa bộ nhớ hệ thống và đòi tiền để giao khóa giải mã (13 chữ cái):

8 hàng ngang: Chương trình được thiết kế để bí mật theo dõi và ghi lại hoạt động và thông tin nhập của người dùng (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Phần mềm độc hại tự nhân bản, lây lan qua mạng mà không cần con người thao tác (10 chữ cái):

2 hàng dọc: Phần mềm độc hại ẩn sâu trong nhân hệ thống để duy trì quyền quản trị (7 chữ cái):

4 hàng dọc: Phần mềm độc hại thực thi trực tiếp trong RAM để tránh bị trình quét ổ đĩa phát hiện (8 chữ cái):

5 hàng dọc: Môi trường ảo tách biệt dùng để phân tích tệp độc hại một cách an toàn (7 chữ cái):

6 hàng dọc: Hạn chế các thiết bị đầu cuối bị nhiễm để ngăn các tải trọng đe dọa lây lan (5 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

T R O J A N G K M M I Ơ Ô E M
M Ơ P Q S R P H E Â S Q Ơ O Ê
H X Q Â U Â C Ô R X P T Â Y U
N O Đ I L Ê Y N B M Y C Ơ Ư Ô
I B Â Ô S Ă A G Y N W C K A C
T D C O C D E T G B A P Ơ L D
Y N G Q Y Q Đ Ê Ơ U R D A A Ơ
A A O M Ô S V P Ơ I E P S T Q
M S B M X Ă Đ Q Ư Ư H A I P Y
U X X K E G M P I L L K R O Ê
Â M A Đ Ô C T Ô N G T I Ê N Ơ
S Ơ E Y A O T Đ T O Â X P X Ă
Ê L Y E H N Ô N O Ư Â L Y X Đ
V O U T K T Ô R Ă N U R L E T
B X T I P Ă Ư Y V L P Ơ V G O

DANH SÁCH TỪ VỰNG

TROJAN MAĐÔCTÔNGTIÊN SPYWARE ROOTKIT SANDBOX CÔLÂP SÂUMAYTINH KHÔNGTỆP

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG
A. TROJAN
B. MAĐÔCTÔNGTIÊN
C. SPYWARE
D. ROOTKIT
E. SANDBOX
F. CÔLÂP
G. SÂUMAYTINH
H. KHÔNGTÊP

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
1. Phần mềm độc hại ẩn sâu trong nhân hệ thống để duy trì quyền quản trị.
2. Hạn chế các thiết bị đầu cuối bị nhiễm để ngăn các tải trọng đe dọa lây lan.
3. Phần mềm độc hại thực thi trực tiếp trong RAM để tránh bị trình quét ổ đĩa phát hiện.
4. Phần mềm độc hại tự nhân bản, lây lan qua mạng mà không cần con người thao tác.
5. Phần mềm độc hại mã hóa bộ nhớ hệ thống và đòi tiền để giao khóa giải mã.
6. Chương trình được thiết kế để bí mật theo dõi và ghi lại hoạt động và thông tin nhập của người dùng.
7. Phần mềm độc hại ngụy trang thành một chương trình tiện ích vô hại hoặc hữu ích.
8. Môi trường ảo tách biệt dùng để phân tích tệp độc hại một cách an toàn.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **OTJANR** _____
2. **SYERAWP** _____
3. **DSBXNOA** _____
4. **YNAHMITSÂU** _____
5. **GIAĐNCNTTÔMÊÔ** _____
6. **IOKRTTO** _____
7. **ÂPCLÔ** _____
8. **NHGPKÊTÔ** _____

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những nơi để tải ứng dụng an toàn			
2	Những thiết bị có thể bị tấn công			
3	Những thứ bạn sao lưu			
4	Những dấu hiệu cảnh báo trong một email			
5	Những dấu hiệu điện thoại có phần mềm độc hại			
6	Những loại phần mềm độc hại bạn biết			
7	Những loại tệp cần cẩn thận			
8	Những cách phần mềm độc hại xâm nhập vào máy tính			
9	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
10	Những từ liên quan đến an ninh mạng			
11	Những việc cần làm sau khi dữ liệu bị rò rỉ			
12	Lý do cập nhật phần mềm			
13	Những con vật hoặc nhân vật có tên giống tên phần mềm độc hại			
14	Những thứ phần mềm độc hại có thể đánh cắp			
15	Những việc cần làm nếu bạn lỡ nhấp vào liên kết sai			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: NGĂN CHẶN MÃ ĐỘC TỐNG TIỀN TRONG DOANH NGHIỆP

👨‍💻

Tình huống: Mạng cục bộ của một doanh nghiệp đã bị ransomware đang hoạt động xâm nhập. Các máy chủ tệp chính đã bắt đầu hiển thị phần mở rộng tệp .locked. Hãy thiết lập các chính sách ngăn chặn.

Câu hỏi thảo luận: Hãy trình bày chi tiết các bước ngăn chặn, và nêu giao thức khôi phục dữ liệu.

NGHIÊN CỨU TÌNH HUỐNG 2: PHẦN MỀM ĐỘC HẠI KHÔNG TỆP CHÈN VÀO BỘ NHỚ

👨‍💻

Tình huống: Một nhà phân tích phát hiện các mẫu kịch bản đáng ngờ đang thực thi trực tiếp trong RAM hệ thống dễ bay hơi bằng các công cụ quản trị tiêu chuẩn, nhưng không có tệp độc hại nào tồn tại trên ổ đĩa.

Câu hỏi thảo luận: Hãy giải thích chiến lược phân tích bộ nhớ, và nêu rõ các công cụ để chặn việc thực thi không dùng tệp.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

20 11 1 24 11 12 9 16 15 1 7 18 5 4 2 16 10

10 12 1 15 23 1 24 11 1 16 11 27 12

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Phần mềm độc hại là gì?

Phần mềm độc hại do các tác nhân đe dọa thiết kế để làm hỏng, chiếm quyền kiểm soát hoặc đánh cắp dữ liệu từ thiết bị và mạng.

Q2: Sự khác biệt giữa virus và sâu máy tính (worm) là gì?

Virus cần có thao tác của con người (như mở tệp) để lây lan, còn sâu máy tính lây lan tự động qua các mạng.

Q3: Trojan lây nhiễm vào máy tính như thế nào?

Nó đánh lừa người dùng bằng cách giả dạng một chương trình vô hại hoặc an toàn, giấu tải trọng độc hại bên trong.

Q4: Ransomware là gì?

Một loại phần mềm độc hại mã hóa các tệp trên hệ thống mục tiêu, đòi tiền để đổi lấy khóa giải mã. [1]

Q5: Phần mềm gián điệp là gì?

Phần mềm độc hại bí mật ghi lại các phím người dùng gõ, mật khẩu và thói quen duyệt web để gửi cho kẻ tấn công.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Sandboxing nghĩa là gì?

Chạy các tệp đáng ngờ trong môi trường ảo an toàn, cô lập để quan sát hành vi của chúng mà không gây rủi ro cho các hệ thống sản xuất.

Q7: Phần mềm độc hại không tệp (fileless) là gì?

Phần mềm độc hại chạy trực tiếp trong bộ nhớ hệ thống (RAM) bằng các tiện ích hợp lệ, tránh ghi tệp xuống đĩa để vượt qua các trình quét cơ bản.

Q8: Rootkit bảo vệ phần mềm độc hại như thế nào?

Nó ẩn các tiến trình và tệp độc hại, thường bằng cách lật đổ nhân hệ điều hành, nên các trình quét diệt virus có thể bỏ sót chúng.

Q9: Giám sát hành vi động là gì?

Quét virus theo dõi các tiến trình đang chạy theo thời gian thực để chặn các hành vi điển hình của phần mềm độc hại, như mã hóa hàng loạt tệp.

Q10: Tại sao việc ngăn chặn là khẩn cấp trong ứng phó sự cố?

Cô lập các điểm cuối bị xâm phạm ngăn các tải trọng phần mềm độc hại đang hoạt động lây lan sang các thiết bị mạng khác.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Các nhà phát triển phần mềm độc hại né các trình quét diệt virus dựa trên chữ ký như thế nào?

Chúng dùng tính đa hình, thay đổi giá trị băm và cấu trúc mã của tệp ở mỗi lần lây nhiễm trong khi vẫn giữ nguyên hành vi độc hại.

Q2: Rủi ro của các công cụ lưỡng dụng trong chiến dịch phần mềm độc hại là gì?

Kẻ tấn công dùng các công cụ quản trị hợp pháp (như PowerShell hoặc Sysinternals) để lẫn vào lưu lượng mạng bình thường, khiến việc phát hiện trở nên khó khăn.

Q3: Process hollowing thực thi mã độc như thế nào?

Nó khởi chạy một tiến trình hệ thống hợp pháp ở trạng thái tạm dừng, thay mã trong bộ nhớ của nó bằng phần mềm độc hại và tiếp tục thực thi.

Q4: Máy chủ chỉ huy và điều khiển (C2) đóng vai trò gì?

Máy chủ từ xa do tin tặc vận hành để gửi chỉ thị và dữ liệu tải đến phần mềm độc hại chạy trên các máy bị xâm nhập.

Q5: Vì sao khó phát hiện keylogging?

Keylogger cơ bản tiêu tốn rất ít tài nguyên CPU và giấu tiến trình của chúng bên trong các tiện ích hợp pháp ở không gian người dùng.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Làm rối mã làm chậm việc phân tích mã độc như thế nào?

Nó mã hóa hoặc sắp xếp lại mã nguồn, khiến công cụ phân tích và trình quét bảo mật không đọc được.

Q7: Chức năng của bootkit là gì?

Rootkit lây nhiễm vào quá trình khởi động (MBR, boot sector hoặc firmware UEFI), nên chạy trước khi hệ điều hành được nạp.

Q8: Quét heuristic nhận diện các mối đe dọa zero-day như thế nào?

Nó quét các mẫu mã đáng ngờ và lệnh quản trị thay vì tìm giá trị băm khớp trong cơ sở dữ liệu.

Q9: Mối đe dọa của DLL hijacking là gì?

Buộc một ứng dụng hợp pháp tải thư viện liên kết động (DLL) độc hại bằng cách đặt nó vào đường dẫn thư mục của ứng dụng.

Q10: Các quy trình phân tích phần mềm độc hại tự động dùng ảo hóa như thế nào?

Chúng chạy các tệp đáng ngờ trên nhiều máy ảo hệ điều hành, tự động tạo nhật ký hành vi và tệp PCAP của mạng.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Trojan vẫn là phương thức lây nhiễm phổ biến vì chúng giấu mã độc bên trong các chương trình trông có vẻ vô hại.

2. THÔNG TIN VỀ AN NINH

IC3 của FBI đã nhận hơn 3.600 khiếu nại về ransomware trong năm 2025, với thiệt hại được báo cáo vượt quá 32 triệu USD. [3]

3. THÔNG TIN VỀ AN NINH

Sâu máy tính có thể lây lan nhanh trên mạng bằng cách khai thác các lỗ hổng giao thức chưa được vá, chẳng hạn EternalBlue trong SMB.

4. THÔNG TIN VỀ AN NINH

Phần mềm độc hại không dùng tệp khó bị phát hiện vì nó chạy trong bộ nhớ thông qua các công cụ hợp lệ và để lại rất ít dấu vết trên ổ đĩa.

5. THÔNG TIN VỀ AN NINH

Các sandbox phân tích thường quay về một ảnh chụp nhanh sạch sau mỗi lần chạy để mỗi bài kiểm tra bắt đầu từ trạng thái đã biết.

6. THÔNG TIN VỀ AN NINH

Rootkit có thể sửa đổi các lời gọi hệ thống của nhân, báo cáo kết quả chẩn đoán sai cho các trình quét phần mềm độc hại.

7. THÔNG TIN VỀ BẢO MẬT

Làm rối mã dùng các tiện ích đóng gói (packer) để nén và che giấu cấu trúc tải nhị phân thực sự của phần mềm độc hại.

8. THÔNG TIN VỀ BẢO MẬT

Phần mềm độc hại đa hình thay đổi mã, và do đó cả giá trị băm tệp, ở mỗi bản sao mới để né kiểm tra chữ ký.

9. THÔNG TIN VỀ BẢO MẬT

Chiếm quyền DLL khai thác cấu hình thứ tự tìm kiếm trong các hệ điều hành phổ biến như Windows.

10. THÔNG TIN VỀ AN NINH

Các nhà cung cấp bảo mật phát hiện số lượng rất lớn mẫu phần mềm độc hại mới mỗi ngày, nên chữ ký cần được cập nhật liên tục.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Đặc điểm nhận dạng của ngựa Trojan (Trojan horse) là gì? → Giả dạng phần mềm hợp pháp để lừa người dùng chạy nó

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Loại phần mềm độc hại nào mã hóa tệp và đòi thanh toán? → Ransomware

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Điều gì đại diện cho phần mềm gián điệp? → Phần mềm độc hại được thiết kế để bí mật theo dõi thao tác gõ phím và hoạt động trình duyệt của người dùng

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Vì sao các nhà phát triển phần mềm độc hại dùng rootkit? → Để che giấu các tiến trình đang chạy và tệp độc hại khỏi hệ điều hành

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Sandboxing nghĩa là gì trong phân tích phần mềm độc hại? → Thực thi các tệp đáng ngờ trong một hầm ảo biệt lập để quan sát hành vi một cách an toàn

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 Câu hỏi 6

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Sai: sâu máy tính tự sao chép và lây lan qua các mạng mà không cần bất kỳ hành động nào của người dùng.

7 Câu hỏi 7

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Sai: phần mềm quảng cáo không phải lúc nào cũng vô hại; phần lớn theo dõi hoạt động duyệt web để nhắm mục tiêu quảng cáo.

8 Câu hỏi 8

Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

Đúng: các bản sao lưu ngoại tuyến sạch khôi phục các tệp bị mã hóa mà không phải trả tiền, dù dữ liệu bị đánh cắp vẫn có thể bị rò rỉ.

9 Câu hỏi 9

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Sai: trình quét theo chữ ký cần một mẫu đã biết, nên phần mềm độc hại zero-day hoàn toàn mới có thể lọt qua chúng.

10 Câu hỏi 10

Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

Phần mềm độc hại không dùng tệp thực thi các tập lệnh độc hại trong bộ nhớ hệ thống, tránh ghi tệp vào ổ đĩa.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

D 1. TROJAN	F 2. RANSOMWARE	A 3. PHẦN MỀM GIÁN ĐIỆP	H 4. ROOTKIT
G 5. SANDBOX	C 6. NGĂN CHẶN	E 7. SÂU MÁY TÍNH	B 8. KHÔNG DÙNG TỆP

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 TROJAN	2 MÃ ĐỘC TỐNG TIỀN	3 PHẦN MỀM GIÁN ĐIỆP	4 ROOTKIT
5 SANDBOX	6 CÔ LẬP		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 D – ROOTKIT	2 F – CÔLẬP	3 H – KHÔNGTỆP	4 G – SÂUMAYTINH
5 B – MAĐỘCTỐNGTIỀN	6 C – SPYWARE	7 A – TROJAN	8 E – SANDBOX

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được TROJAN, RANSOMWARE và PHẦN MỀM GIÁN ĐIỆP bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

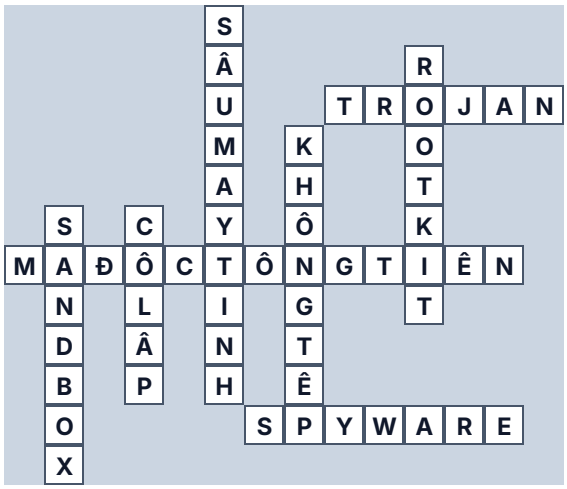
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

T	R	O	J	A	N	G	K	M	M	I	Ơ	Ô	E	M
M	Ơ	P	Q	S	R	P	H	E	Â	S	Q	Ơ	O	Ê
H	X	Q	Â	U	Â	C	Ô	R	X	P	T	Â	Y	U
N	O	Đ	I	L	Ê	Y	N	B	M	Y	C	Ơ	Ư	Ô
I	B	Â	Ô	S	Ă	A	G	Y	N	W	C	K	A	C
T	D	C	O	C	D	E	T	G	B	A	P	Ơ	L	D
Y	N	G	Q	Y	Q	Đ	Ê	Ơ	U	R	D	A	A	Ơ
A	A	O	M	Ô	S	V	P	Ơ	I	E	P	S	T	Q
M	S	B	M	X	Ă	Đ	Q	Ư	Ư	H	A	I	P	Y
U	X	X	K	E	G	M	P	I	L	L	K	R	O	Ê
Â	M	A	Đ	Ô	C	T	Ô	N	G	T	I	Ê	N	Ơ
S	Ơ	E	Y	A	O	T	Đ	T	O	Â	X	P	X	Ă
Ê	L	Y	E	H	N	Ô	N	O	Ư	Â	L	Y	X	Đ
V	O	U	T	K	T	Ô	R	Ă	N	U	R	L	E	T
B	X	T	I	P	Ă	Ư	Y	V	L	P	Ơ	V	G	O

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: TROJAN Phần mềm độc hại ngụy trang thành một chương trình tiện ích vô hại hoặc hữu ích (6 chữ cái)

7 hàng ngang: MAĐÔCTÔNGTIÊN Phần mềm độc hại mã hóa bộ nhớ hệ thống và đòi tiền để giao khóa giải mã (13 chữ cái)

8 hàng ngang: SPYWARE Chương trình được thiết kế để bí mật theo dõi và ghi lại hoạt động và thông tin nhập của người dùng (7 chữ cái)

HÀNG DỌC

1 hàng dọc: SÂUMAYTINH Phần mềm độc hại tự nhân bản, lây lan qua mạng mà không cần con người thao tác (10 chữ cái)

2 hàng dọc: ROOTKIT Phần mềm độc hại ẩn sâu trong nhân hệ thống để duy trì quyền quản trị (7 chữ cái)

4 hàng dọc: KHÔNGTÊP Phần mềm độc hại thực thi trực tiếp trong RAM để tránh bị trình quét ổ đĩa phát hiện (8 chữ cái)

5 hàng dọc: SANDBOX Môi trường ảo tách biệt dùng để phân tích tệp độc hại một cách an toàn (7 chữ cái)

6 hàng dọc: CÔLÂP Hạn chế các thiết bị đầu cuối bị nhiễm để ngăn các tải trọng đe dọa lây lan (5 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1.	OTJANR	TROJAN	5.	GIAĐNCNTTÔMÊÔ	MAĐÔCTÔNGTIÊN
2.	SYERAWP	SPYWARE	6.	IOKRTTO	ROOTKIT
3.	DSBXNOA	SANDBOX	7.	ÂPCLÔ	CÔLÂP
4.	YNAHMITSÂU	SÂUMAYTINH	8.	NHGPKÊTÔ	KHÔNGTÊP

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"PHAT HIÊN MA ĐÔC BĂNG GIAM SAT HANH VI"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Ngăn chặn mã độc tống tiền trong doanh nghiệp

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Mạng cục bộ của một doanh nghiệp đã bị ransomware đang hoạt động xâm nhập. Các máy chủ tệp quan trọng bắt đầu hiển thị phần mở rộng tệp .locked. Hãy thiết lập các chính sách ngăn chặn.
- Chiến lược và giải pháp đề xuất: Ngắt kết nối tất cả máy chủ bị ảnh hưởng khỏi mạng cục bộ. Chấm dứt các phiên quản trị đang hoạt động. Khôi phục các tệp chưa bị xâm phạm từ hệ thống sao lưu ngoại tuyến an toàn, bị khóa ghi.

B Nghiên cứu tình huống 2: Phần mềm độc hại không tệp chèn vào bộ nhớ

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một nhà phân tích phát hiện các mẫu script đáng ngờ chạy trực tiếp trong RAM hệ thống tạm thời bằng các công cụ quản trị tiêu chuẩn, nhưng không có tệp độc hại nào trên ổ đĩa.
- Chiến lược và giải pháp đề xuất: Cô lập các điểm cuối bị ảnh hưởng và chụp ảnh bộ nhớ trước. Xem lại nhật ký PowerShell và WMI, chặn các tập lệnh chưa được phê duyệt bằng AppLocker, rồi khởi động lại để xóa mã độc.