TẤN CÔNG & PHÒNG THỦ HỆ THỐNG

Module 8. DoS/DDoS Attack

1. Tổng quan
2. Một số kỹ thuật tấn công DoS/DDoS
3. Giải pháp phòng chống

1. Tổng quan
2. Một số kỹ thuật tấn công DoS/DDoS
3. Giải pháp phòng chống

What is a DoS Attack?

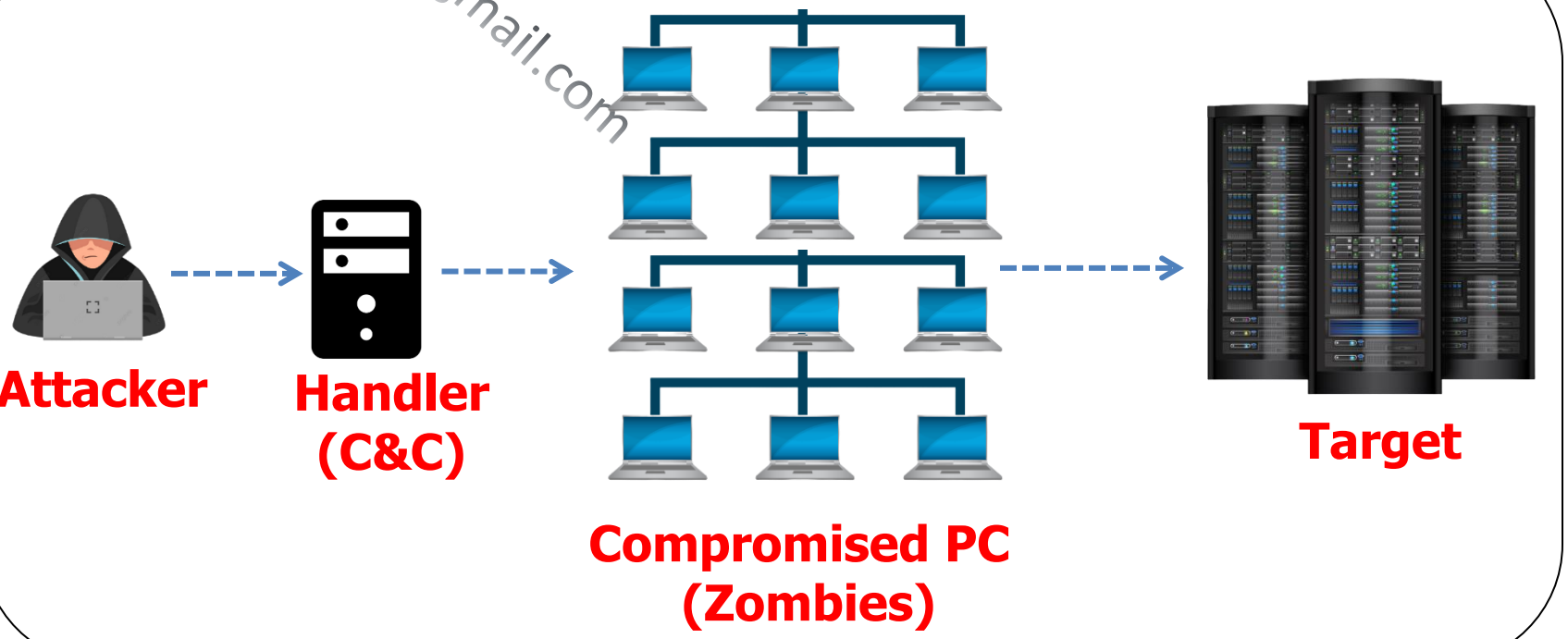
- Tấn công từ chối dịch vụ (Denial of Service) là một cuộc tấn công vào một máy tính hoặc một hệ thống nhằm làm giảm, hạn chế hoặc ngăn chặn khả năng truy cập tài nguyên hệ thống đối với người dùng hợp lệ.
  - Làm quá tải băng thông, tài nguyên hệ thống, khả năng xử lý của dịch vụ.
  - Làm "crash" dịch vụ hoặc phá hủy tập tin, thay đổi thành phần cấu trúc mạng.

What is a DDoS Attack?

❑ Tấn công từ chối dịch vụ phân tán (Distributed DoS) là một cuộc tấn công phối hợp gồm nhiều hệ thống bị chiếm quyền (Botnet) thực hiện tấn công một mục tiêu duy nhất, do đó gây ra gián đoạn dịch vụ cho người dùng hợp lệ.

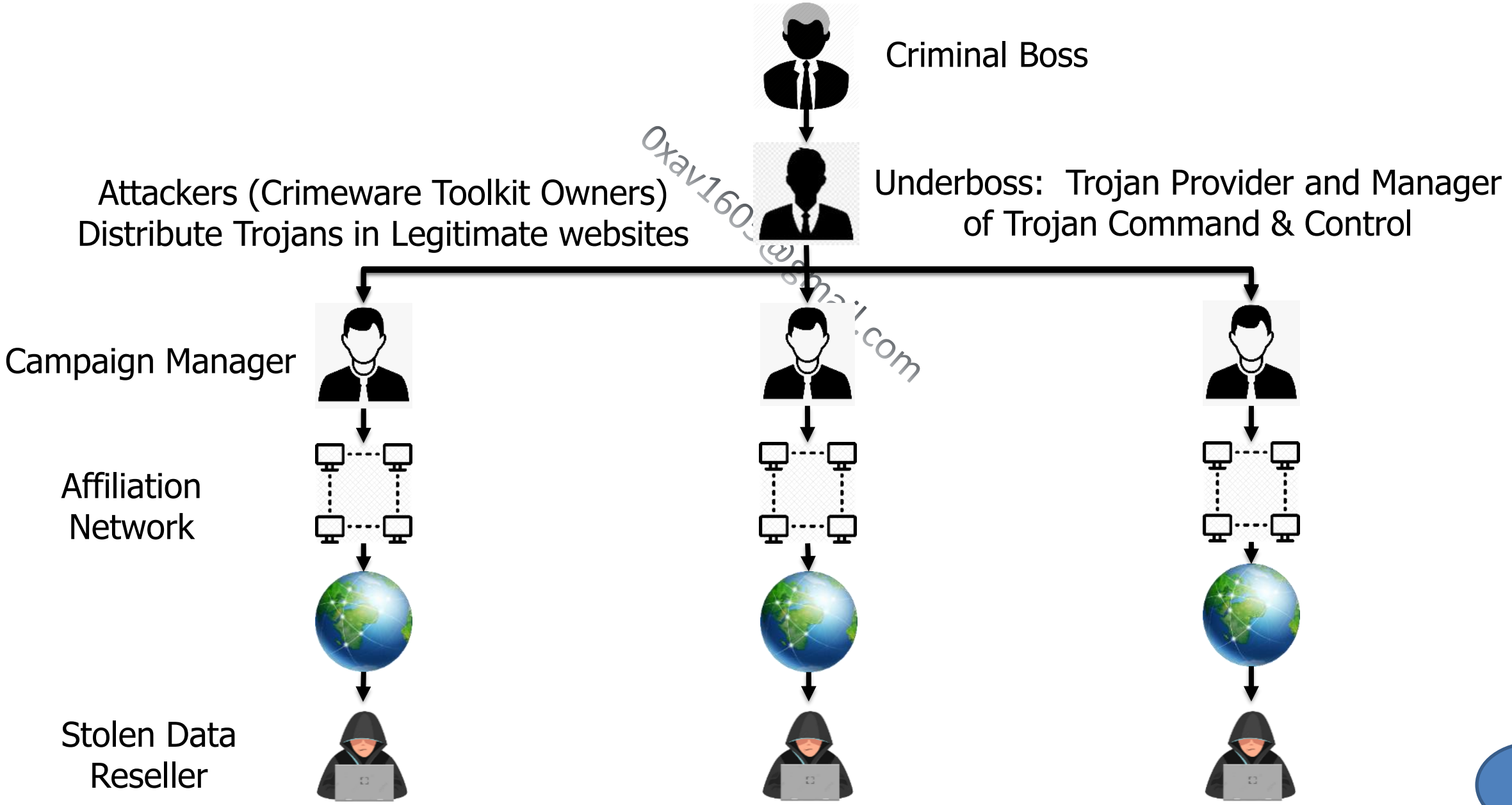
Ảnh hưởng của DDoS

- Mất tính sẵn sàng
- Mạng bị vô hiệu hóa
- Tổn thất tài chính
- Thiệt hại cho tổ chức



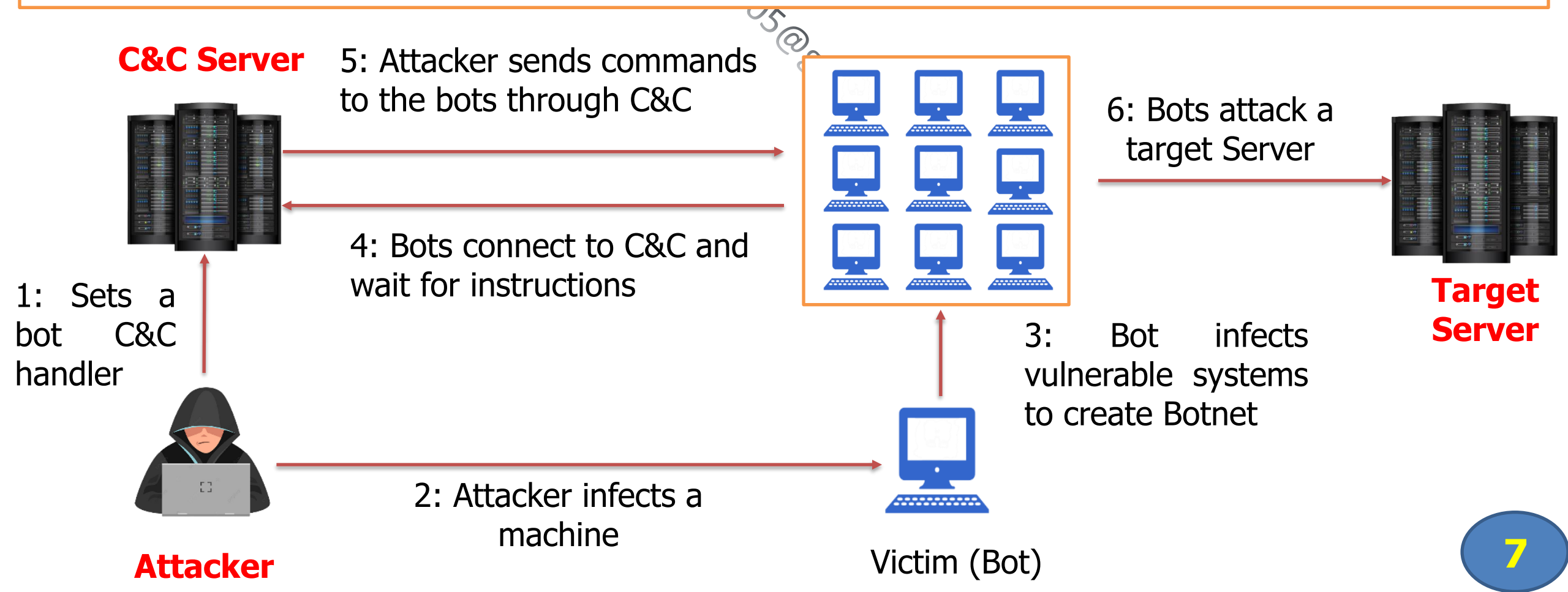
Cách thức hoạt động của DDoS

Organized Cyber Crime: Organizational Chart

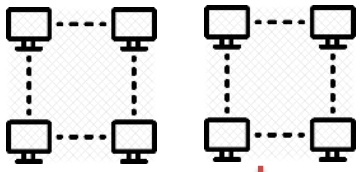


Botnets

- Bots là các phần mềm tự động thực hiện tác vụ qua Internet.
- Botnet là một mạng khổng lồ các hệ thống bị chiếm quyền điều khiển và có thể bị attacker sử dụng để khởi động các cuộc tấn công khác nhau.



A Typical Botnet Setup



Affiliation Network

2: Recruits affiliates

Attacker

3: Affiliates contribute malware

1: Sets a C&C center and Crimeware Toolkit Database (CTD)

5: Redirect victims to malicious website using SE

4: Compromise legitimate website or create new malicious website

8: Malware infects user systems

9: Bots connect back to C&C

10: Bots will receive instructions from C&C to attack primary target

7: Malicious website redirects users to the CTD

Malicious Website

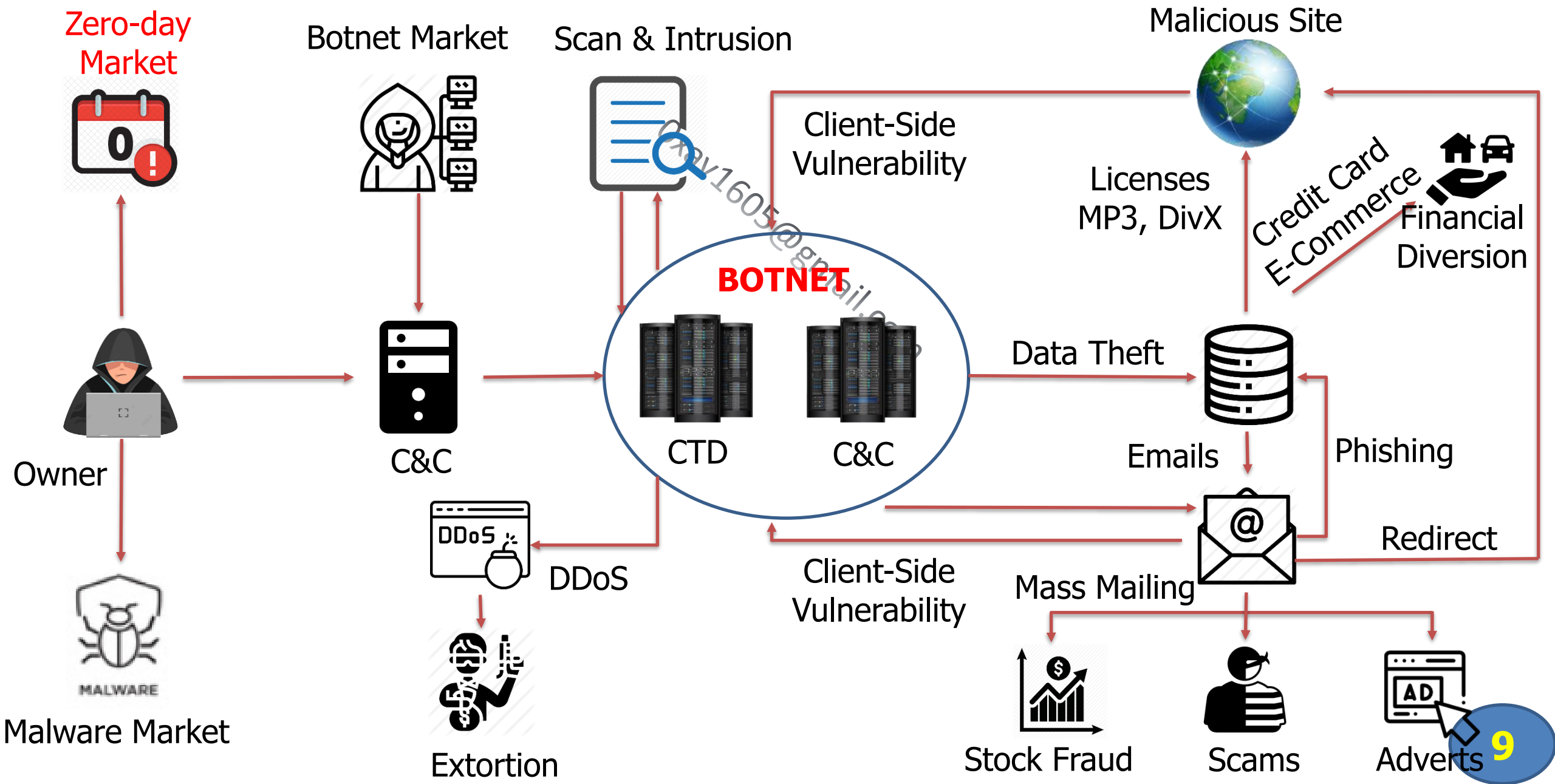
6: User visit the malicious website

Victims

Ogranization

11: Attack the primary target

Botnet Ecosystem



Scanning Methods for Finding Vulnerable Machines

Random Scanning	• Máy bị nhiễm sẽ thăm dò địa chỉ IP ngẫu nhiên từ dải IP mạng mục tiêu và kiểm tra lỗ hổng.
Hit-list Scanning	• Kẻ tấn công trước tiên sẽ thu thập danh sách các máy có dễ bị tổn thương và sau đó dò quét chúng.
Topological Scanning	• Sử dụng thông tin thu được trên máy bị nhiễm để tìm các máy mới dễ bị tổn thương.
Local Subnet Scanning	• Máy bị nhiễm sẽ tìm các máy mới dễ bị tổn thương trong mạng cục bộ của chính nó.
Permutation Scanning	• Sử dụng danh sách hoán vị giả ngẫu nhiên của các địa chỉ IP để tìm các máy mới dễ bị tổn thương.

How Does Malicious Code Propagate? (1/2)

❑ Attacker thường sử dụng ba kỹ thuật để phát tán mã độc hại

Central Source Propagation

❑ Attacker đặt bộ công cụ tấn công vào nguồn trung tâm và một bản sao được chuyển đến hệ thống dễ bị tấn công mới được phát hiện.

Back-chaining Propagation

❑ Attacker đặt bộ công cụ tấn công trên chính hệ thống của mình và một bản sao được chuyển đến hệ thống dễ bị tổn thương mới được phát hiện.

Autonomous Propagation

❑ Máy chủ tấn công tự chuyển bộ công cụ tấn công sang hệ thống dễ bị tổn thương mới được phát hiện tại thời điểm nó xâm nhập vào hệ thống đó.

How Does Malicious Code Propagate? (2/2)

Central Source Propagation

Back-chaining Propagation

Autonomous Propagation

1. Tổng quan
2. Một số kỹ thuật tấn công DoS/DDoS
3. Giải pháp phòng chống

Basic Categories of DoS/DDoS Attack Vectors (1/3)

Volumetric Attacks

- Tiêu thụ băng thông của mạng hoặc dịch vụ mục tiêu.
- Mức độ tấn công đo bằng bits-per-sec (bps).
- Các kiểu tấn tấn công:
  - Tấn công flood.
  - Tấn công khuyếch đại.

Attack Techniques

- UDP flood attack
- ICMP flood attack
- Smuft và Ping of Death attack
- 0-day attack

Basic Categories of DoS/DDoS Attack Vectors (2/3)

Protocol Attacks

- Sử dụng các loại tài nguyên khác như bảng trạng thái kết nối (connection state tables) trong các thành phần hạ tầng mạng như bộ cân bằng tải, tường lửa và máy chủ ứng dụng
- Mức độ tấn công đo bằng packets-per-second (pps)

Attack Techniques

- SYN flood attack
- Segmentation attack
- Spoofed session flood attack
- ACK flood attack
- TCP SACK panic attack

Basic Categories of DoS/DDoS Attack Vectors (3/3)

Application Layer Attacks

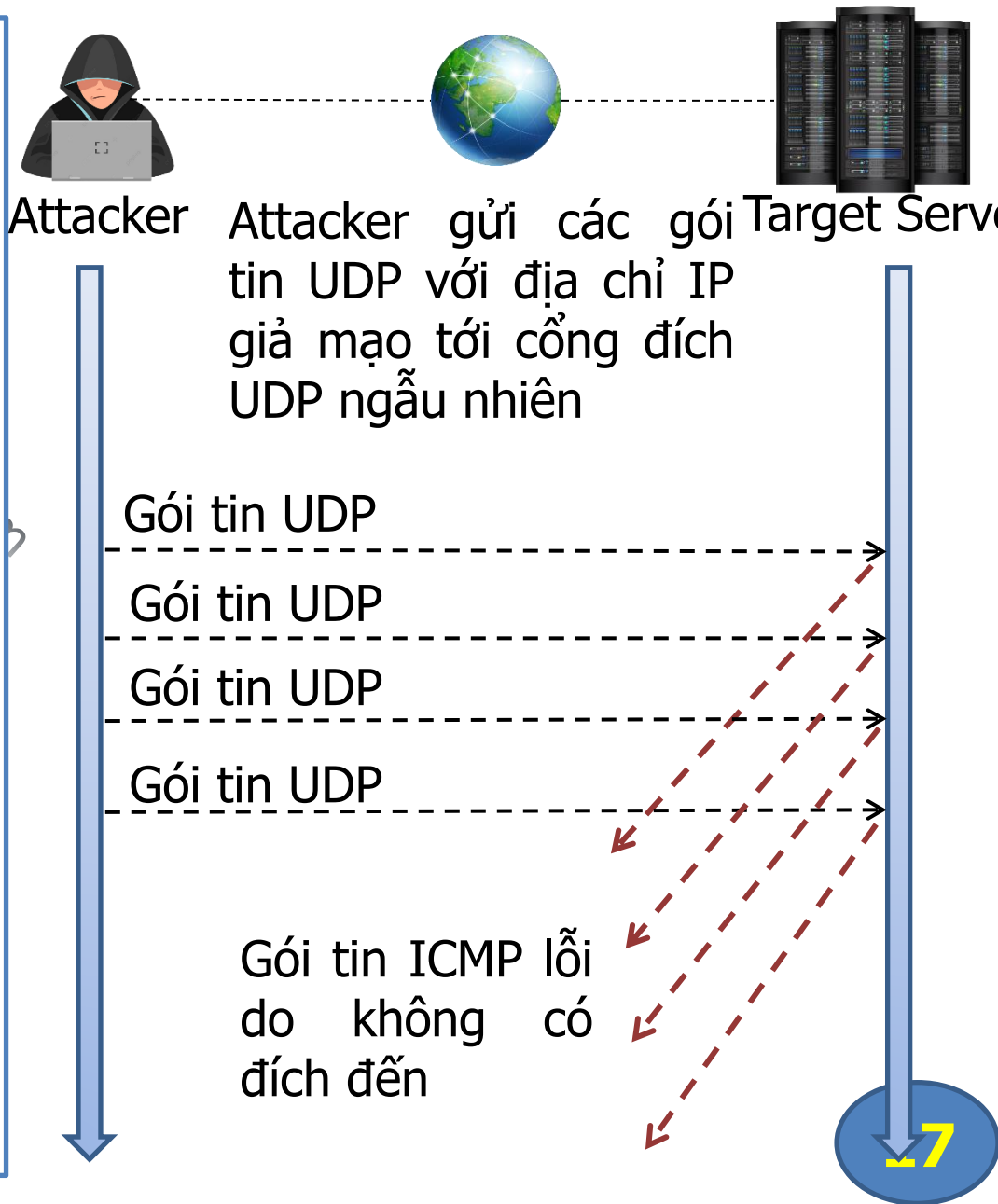
- Tiêu thụ tài nguyên của dịch vụ hoặc ứng dụng khiến cho nó không khả dụng với người dùng hợp lệ.
- Mức độ tấn công được đo bằng request-per-second (rps).

Attack Techniques

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer attack
- DDoS extortion attack

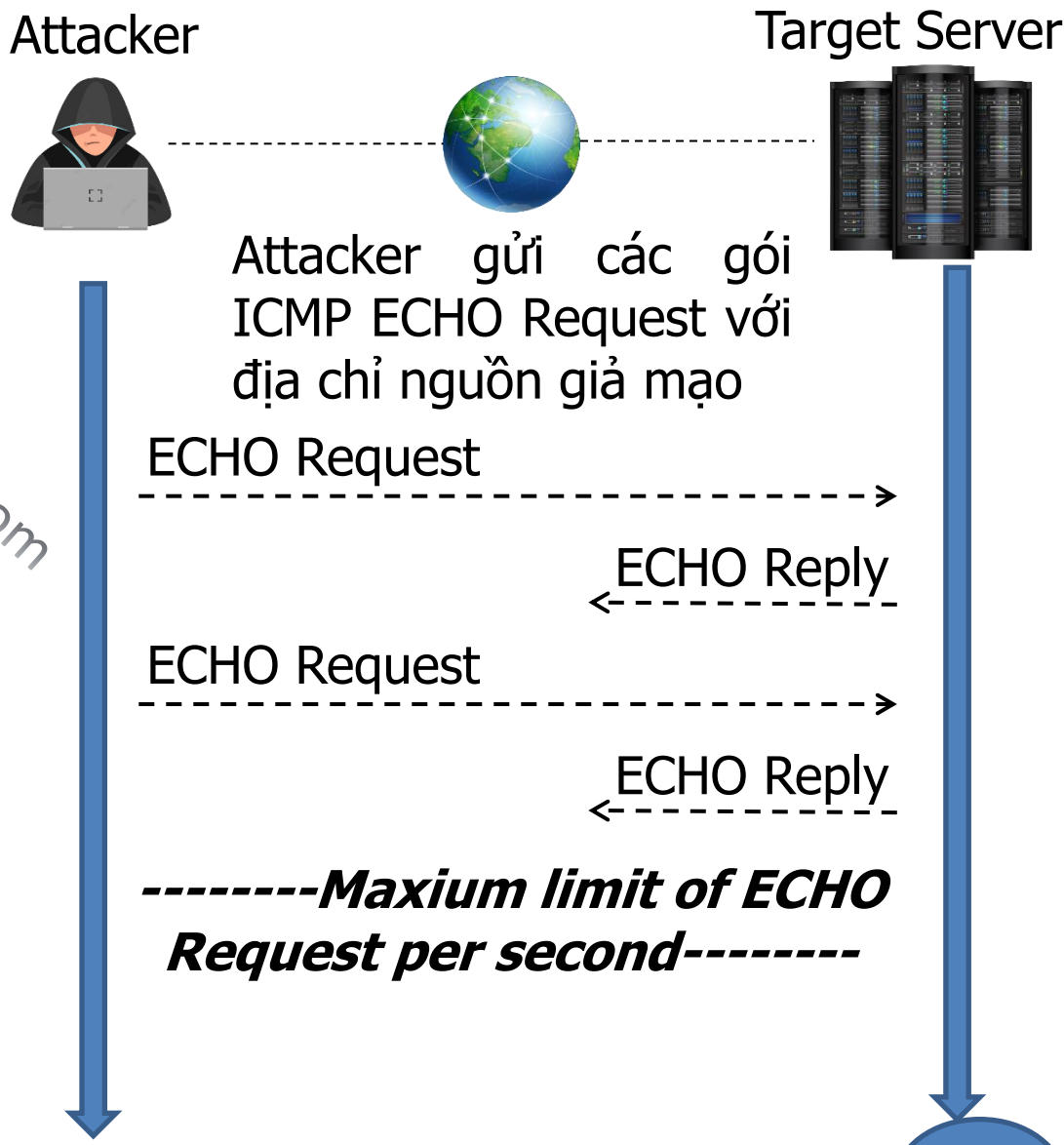
UDP Flood Attack

- Attacker gửi liên tục các gói UDP giả mạo đến máy chủ từ xa trên các cổng ngẫu nhiên.
- Máy chủ liên tục phải kiểm tra các ứng dụng không tồn tại ở các cổng.
- Ứng dụng hợp lệ không thể truy cập và hệ thống đưa ra phản hồi với gói ICMP "Destination Unreachable".
- Tấn công này tiêu thụ tài nguyên mạng và băng thông, làm cho cạn kiệt mạng đến khi hệ thống bị sập.



ICMP Flood Attack

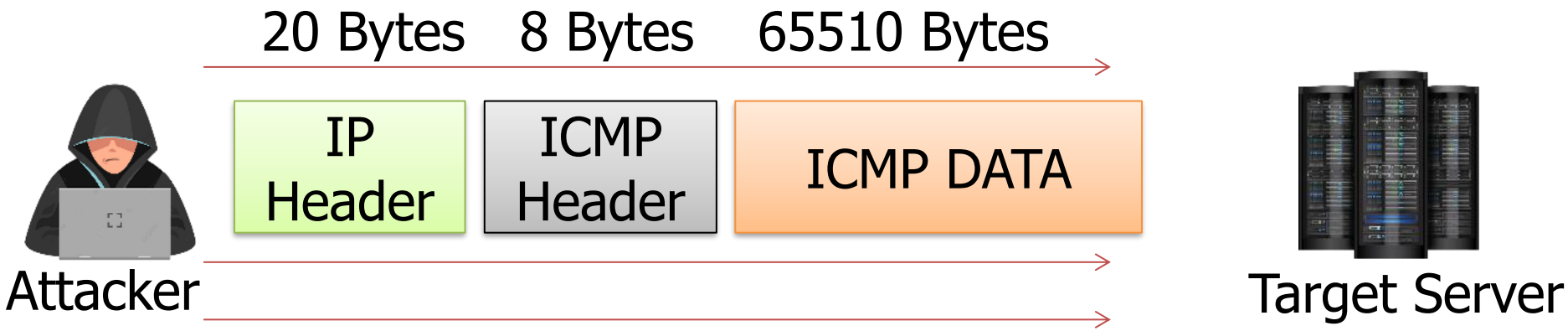
- Quản trị viên thường dùng ICMP cho các hoạt động khắc phục sự cố.
- Tấn công ICMP flood - kẻ tấn công gửi liên tiếp một số lượng lớn các gói ICMP ECHO Request đến hệ thống nạn nhân một cách trực tiếp hoặc gián tiếp khiến máy nạn nhân bị quá tải và ngừng phản hồi các yêu cầu TCP/IP hợp lệ.
- Để bảo vệ khỏi cuộc tấn công này, ta cần đặt ngưỡng giới hạn (1000 packets/sec).



Ping of Death (PoD)

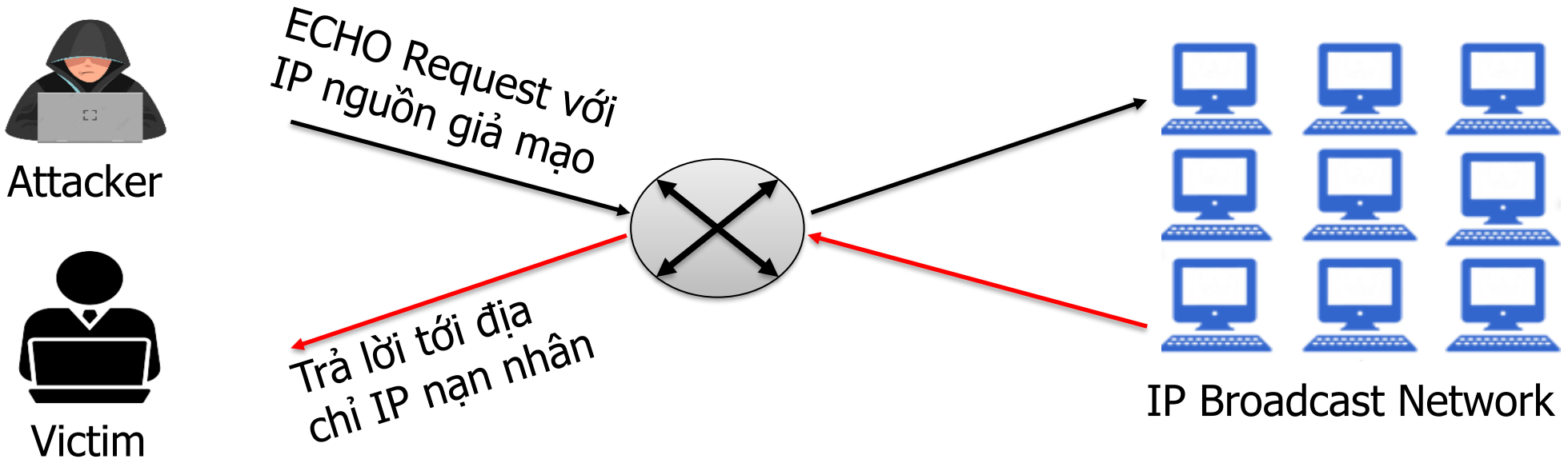
❑ Trong tấn công PoD, attacker gửi các gói tin không đúng định dạng hoặc quá lớn bằng cách sử dụng một lệnh ping đơn giản tới mục tiêu.

❑ Ví dụ: Attacker gửi các gói tin có kích thước 65.538 byte cho máy chủ web mục tiêu. Kích thước này của gói tin vượt giới hạn kích thước do RFC 791 IP quy định là 65,535 byte. Việc lắp ráp lại gói tin có thể khiến hệ thống bị "crassh".



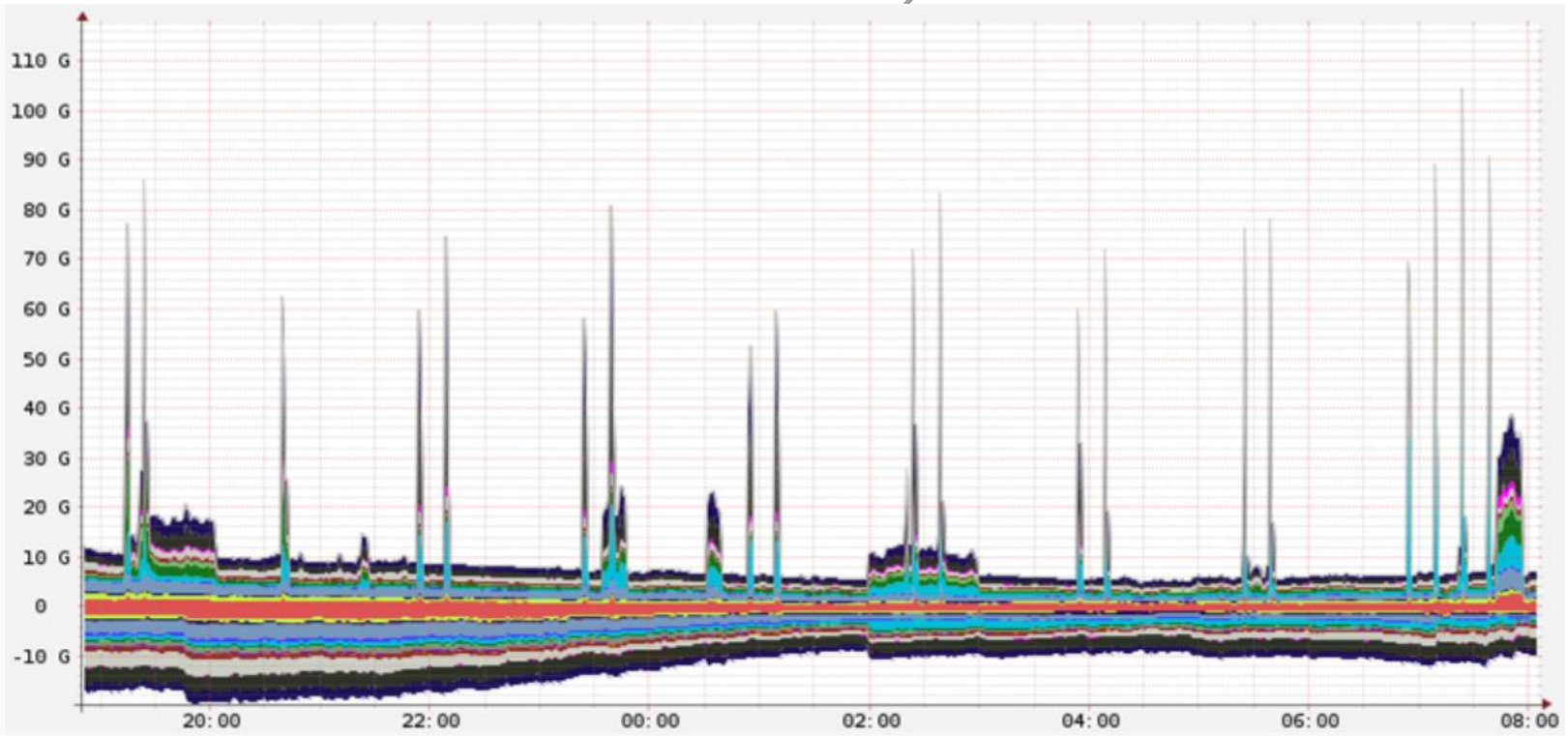
Smurf Attack

- Trong cuộc tấn công Smurf, attacker giả mạo địa chỉ lP nguồn với địa chỉ IP của nạn nhân và gửi nhiều gói ICMP ECHO Request đến mạng IP broadcast.
- Điều này khiến tất cả các máy chủ trên mạng cần phản hồi lại các yêu cầu ICMP ECHO request nhận được. Những phản hồi này sẽ được gửi đến máy nạn nhân và có thể gây ra "crash".



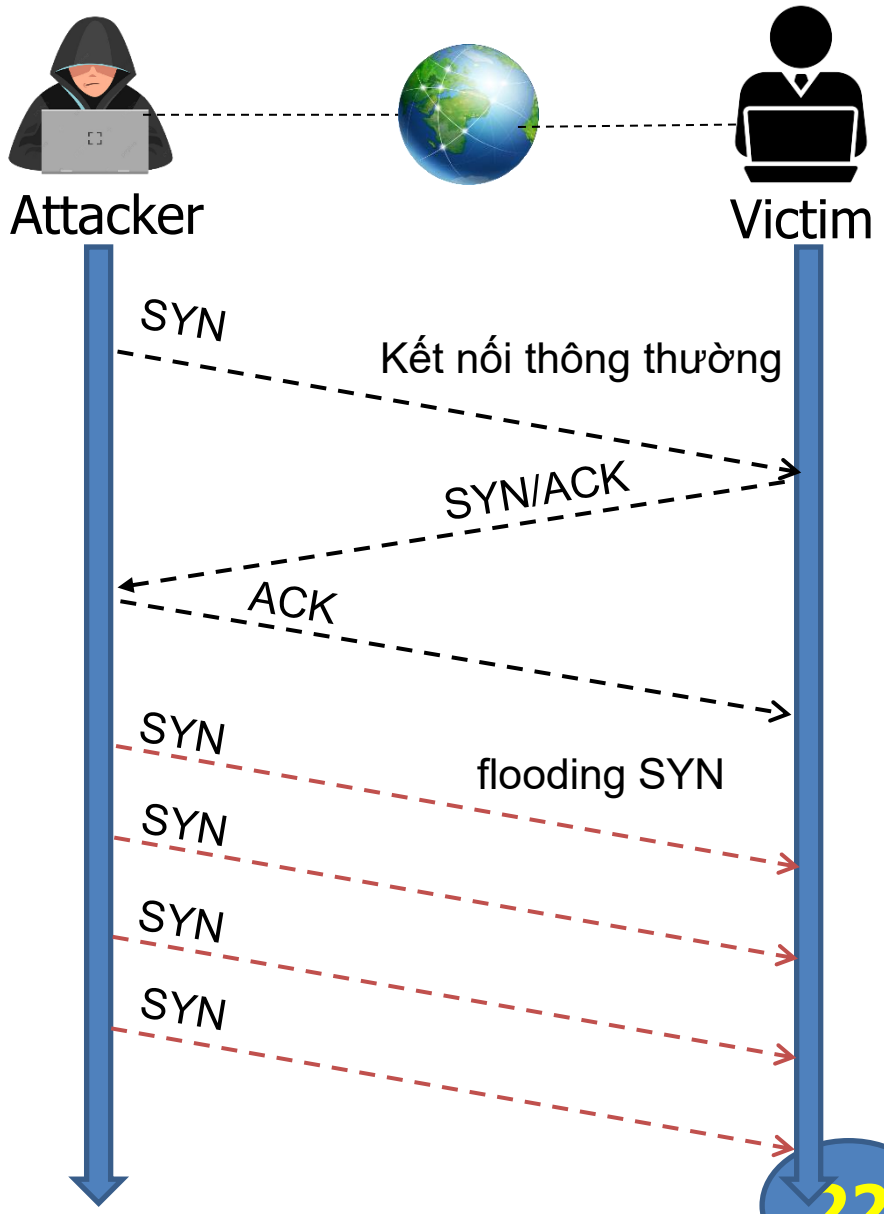
Pulse wave DDoS Attack

- Trong tấn công này, attacker gửi một chuỗi các gói định kỳ, lặp đi lặp lại dưới dạng "xung" đến mục tiêu cứ sau mỗi khoảng thời gian nhất định và mỗi phiên tấn công cụ thể có thể kéo dài vài giờ cho đến vài ngày.
- Xung đơn (single pulse) từ 300 Gbps trở lên là đủ để làm tắc nghẽn mạng.



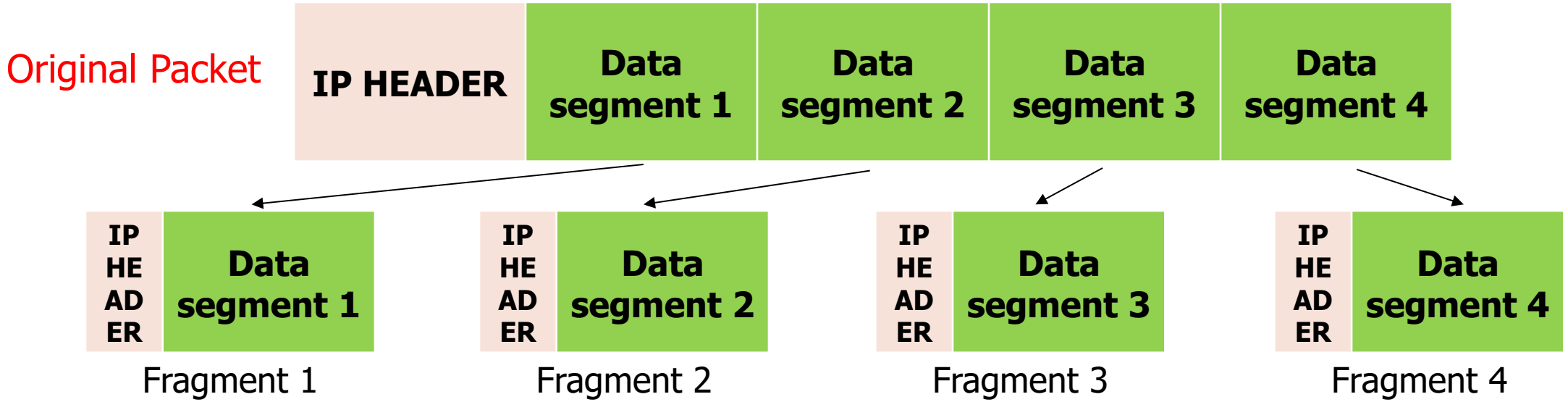
SYN Flood Attack

- Attacker gửi số lượng lớn SYN request đến máy nạn nhân sử dụng IP nguồn giả mạo.
- Máy nạn nhân sẽ gửi lại một SYN ACK để phản hồi lại yêu cầu và đợi ACK trong ít nhất 75 giây để hoàn thành thiết lập phiên.
- Máy nạn nhân không nhận được phản hồi vì IP nguồn là giả mạo.
- Attacker có thể khai thác bằng cách gửi nhiều yêu cầu SYN đến mục tiêu dẫn tới hàng đợi của nạn nhân nhanh chóng bị lấp đầy.



Fragmentation Attack

- Các cuộc tấn công này phá hủy khả năng "re-assemble fragmented packets" bằng cách gửi một số lượng lớn các gói bị phân mảnh (1500+ byte) đến máy chủ mục tiêu. Việc lắp ráp và kiểm tra lại các gói tin bị phân mảnh này tiêu tốn "rất" nhiều tài nguyên (do gói tin bị mã hóa, bị sai kích thước…).
- Vì giao thức cho phép "phân mảnh" nên các gói này thường đi qua các thiết bị mạng như router, firewall, IDS/IPS.



Spoofed Session Flood Attack

- Attacker tạo phiên TCP giả mạo bằng cách gửi nhiều gói SYN, ACK, RST hoặc FIN.
- Attacker sử dụng cách tấn công này để bypass FW và thực hiện tấn công DDoS.

Multiple SYN-ACK Spoofed Session Flood Attack

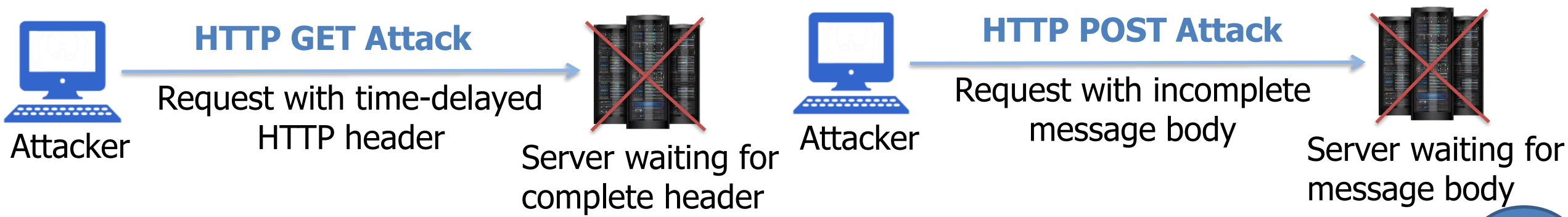
- Attacker tạo phiên giả mạo với nhiều gói SYN và nhiều gói ACK cùng với một hoặc nhiều gói RST hoặc FIN

Multiple ACK Spoofed Session Flood Attack

- Attacker tạo phiên giả mạo bằng cách bỏ qua hoàn toàn các gói SYN và chỉ sử dụng nhiều gói ACK cùng với một hoặc nhiều gói RST hoặc FIN

HTTP GET/POST

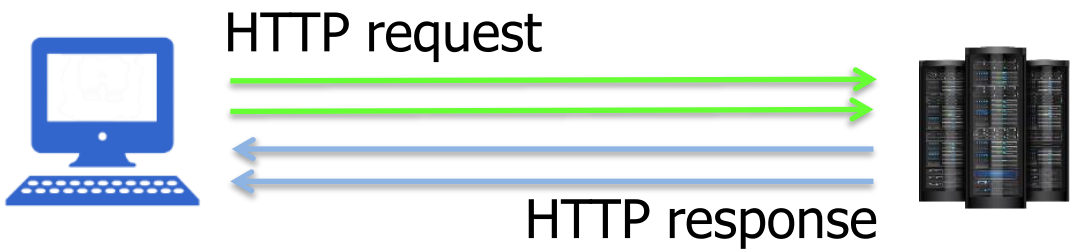
- HTTP Clients (web browsers) kết nối với web server thông qua giao thức HTTP để gửi HTTP request (GET/POST).
- Trong tấn công HTTP GET, attacker sử dụng time-delayed HTTP header để duy trì các kết nối HTTP và làm cạn kiệt tài nguyên máy chủ web.
- Trong tấn công HTTP POST, attacker gửi các HTTP request với header hoàn chỉnh nhưng nội dung lại không hoàn chỉnh làm cho Web server đợi phần còn lại của nội dung request.



Slowloris Attack

- Trong tấn công Slowloris, attacker sẽ mở nhiều kết nối đến mục tiêu bằng cách gửi nhiều nhiều "partial HTTP request header".
- Khi nhận được các "partial HTTP request header", máy chủ mục tiêu sẽ mở nhiều kết nối và tiếp tục chờ các "request" được hoàn thành.
- Các "request" này sẽ không hoàn thành và kết quả là nhóm kết nối đồng thời tối đa của máy chủ mục tiêu sẽ được lấp đầy và lần thử kết nối bổ sung sẽ bị loại bỏ.

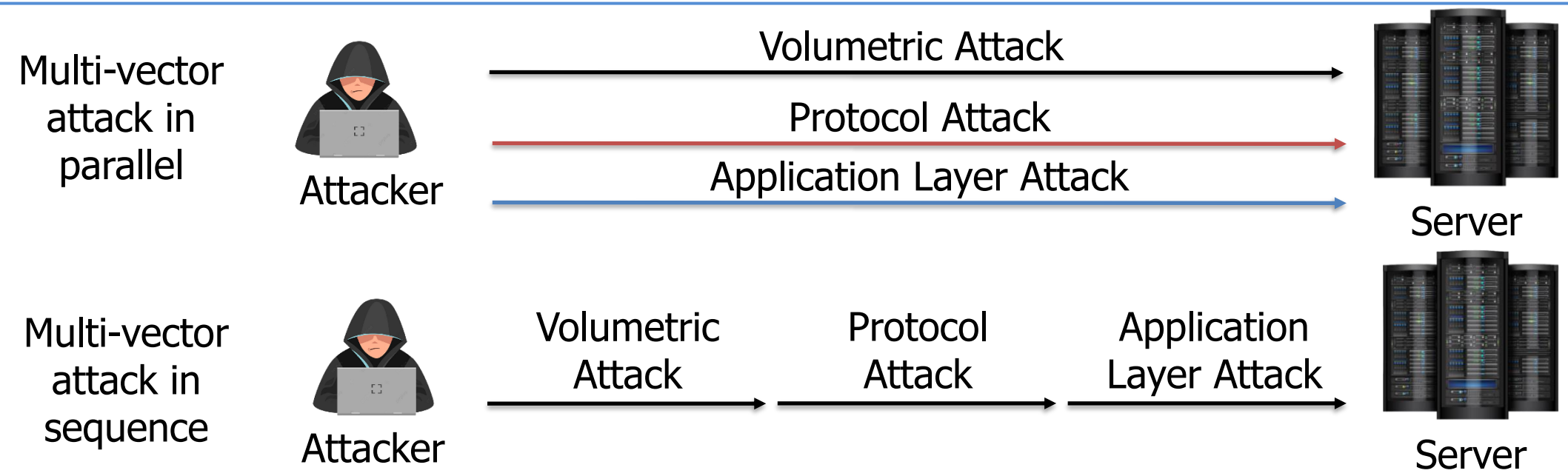
Normal HTTP request-response connection



Slowloris DDoS Attack

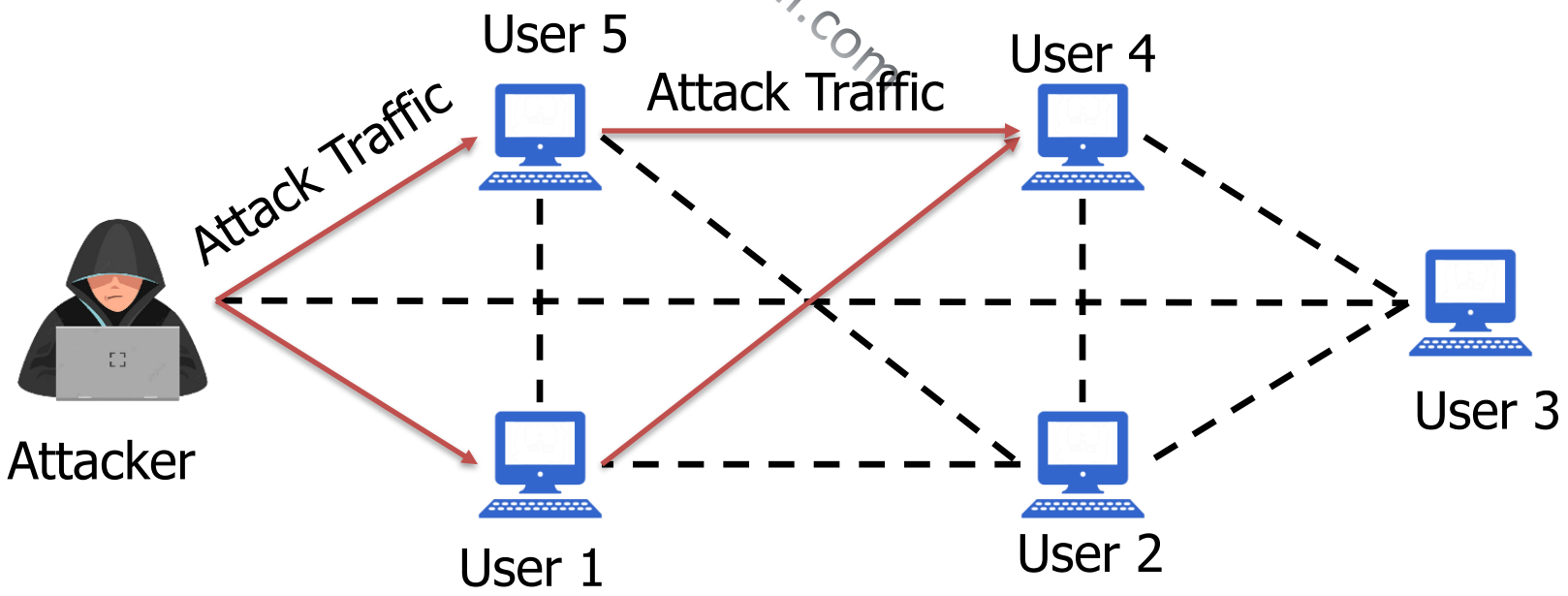
Multi-Vector Attack

- Multi-vector attack (tấn công đa vector) là hình thức phức tạp nhất trong các dạng DDoS, trong đó attacker sử dụng kết hợp các cuộc tấn công theo lưu lượng, giao thức và tầng ứng dụng.
- Attacker nhanh chóng thay đổi từ dạng tấn công DDoS này sang dạng khác (ví dụ từ SYN sang layer-7) hoặc thực hiện đồng thời khiến cho việc phòng chống trở nên khó khăn.



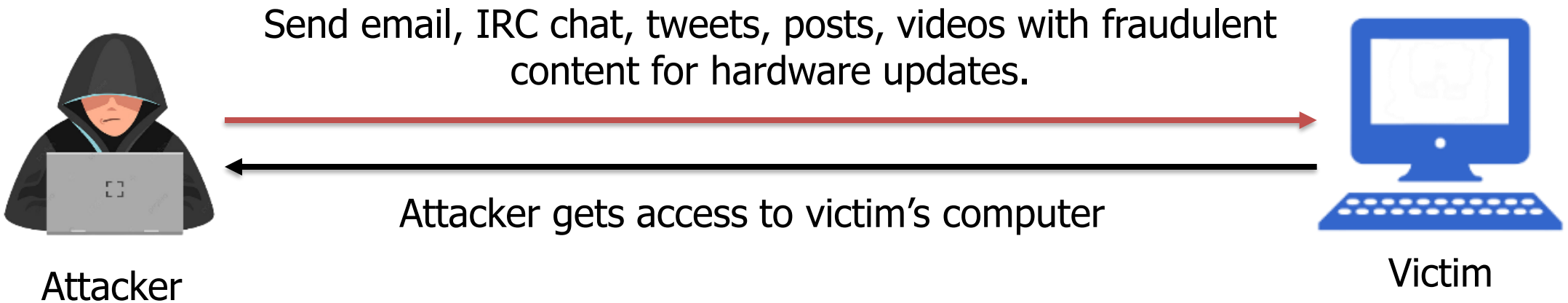
Peer-to-Peer Attack

- Attacker chỉ thị cho máy khách ngắt kết nối khỏi mạng ngang hàng của chúng và kết nối với máy nạn nhân.
- Attacker khai thác các lỗ hổng trong mạng sử dụng giao thức DC++ (Direct Connect) được sử dụng để chia sẻ tất cả các loại tệp giữa các máy khách.



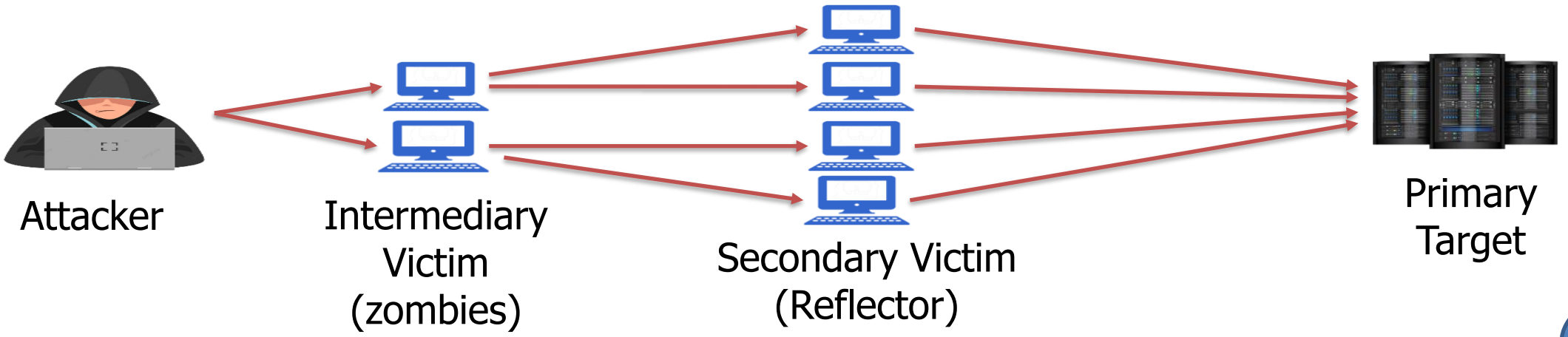
Permanent Denial of Service Attack (PDoS)

- PDoS (a.k.a phlashing) - đề cập đến các cuộc tấn công gây ra thiệt hại không thể phục hồi cho phần cứng hệ thống.
- Không giống như các cuộc tấn công DoS khác, PDoS phá hoại phần cứng hệ thống, yêu cầu nạn nhân thay thế hoặc cài đặt lại phần cứng.
- Attacker gửi cho nạn nhân bản cập nhật phần cứng giả mạo để "phlashing" firmware của thiết bị nạn nhân.



Distributed Reflection DoS (DRDoS) Attack

- Attacker gửi các yêu cầu đến nhiều máy chủ trung gian, các yêu cầu này sau đó được chuyển đến các máy chủ thứ cấp để phản xạ lưu lượng tấn công tới hệ thống mục tiêu.
- Attacker ra lệnh cho zombies gửi các gói tin (TCP SYN) với IP nguồn là IP của nạn nhân tới Reflectors. Kết quả là Reflector gửi một lượng lớn SYN/ACK tới máy nạn nhân. Nạn nhân sẽ loại bỏ các gói SYN/ACK này và Reflector sẽ tiếp tục gửi lại các gói SYN/ACK này cho tới khi thời gian chờ kết thúc.



DoS/DDoS Attack Tools

- High Orbit Ion Cannon(HOIC) – có khả năng nhắm nhiều mục tiêu cùng lúc (URL, domain…)
- Low Orbit Ion Cannon (LOIC) – mục tiêu đơn lẻ
- HULK
- Slowloris
- Metasploit
- https://github.com/topics/ddos-attack-tools

1 Tổng quan

2 Một số kỹ thuật tấn công DoS/DDoS

3 Giải pháp phòng chống

Detection Techniques

- Các kỹ thuật phát hiện dựa trên việc xác định và phân biệt sự gia tăng lưu lượng bất hợp pháp, xác định độ lệch bất thường và đáng chú ý so với lưu lượng mạng thông thường.
- Một số kỹ thuật phát hiện:
  - Activity Profiling
  - Sequential Change-Point Detection
  - Wavelet-Based Signal Analysis

DoS/DDoS Countermeasure Strategies

Hấp thụ tấn công	• Sử dụng nguồn lực bổ sung để hấp thụ tấn công • Yêu cầu lên kế hoạch từ trước và tài nguyên bổ sung
Hạ cấp dịch vụ	• Xác định và giữ cho các dịch vụ quan trọng hoạt động và dừng các dịch vụ không quan trọng
Tắt các dịch vụ	• Tắt tất cả các dịch vụ cho đến khi cuộc tấn công lắng xuống

DoS/DDoS Attack Countermeasure

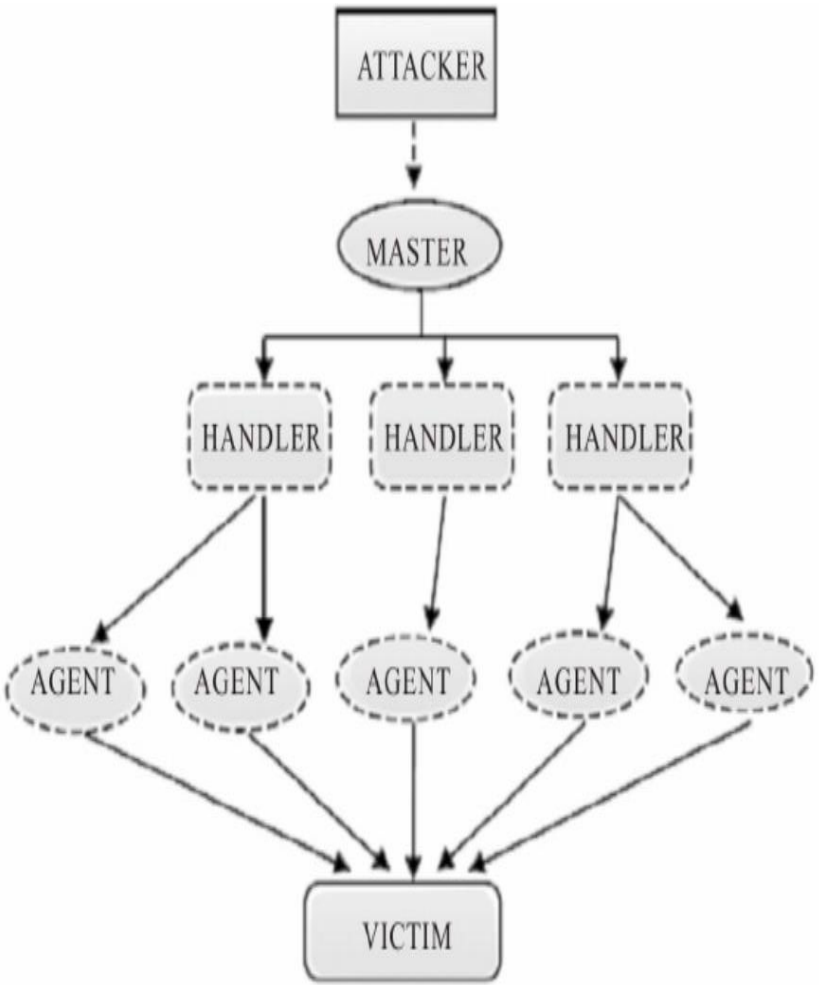
1	Bảo vệ nạn nhân thứ cấp
2	Phát hiện và vô hiệu hóa “Handler”
3	Ngăn chặn các tấn công tiềm ẩn
4	Làm lệch hướng tấn công
5	Giảm thiểu tấn công
6	Điều tra hậu tấn công

Protect Secondary Victims

- Giám sát bảo mật thường xuyên để luôn được bảo vệ khỏi DDoS agent.
- Cài đặt và cập nhật thường xuyên Antivirus.
- Nâng cao nhận thức về ATTT và các kỹ thuật phòng ngừa ở tất cả người dùng internet.
- Tắt các dịch vụ không cần thiết, gỡ cài đặt các ứng dụng không sử dụng và quét tất cả các tệp nhận được từ các nguồn bên ngoài.
- Đảm bảo việc cấu hình đúng cách và cập nhật thường xuyên các cơ chế bảo vệ được tích hợp trong phần cứng và phần mềm cốt lõi của hệ thống.

Detect and Neutralize Handler

- **Phân tích lưu lượng mạng** - phân tích các giao tức truyền thông và các mẫu lưu lượng giữa handlers và clients hoặc handlers và agent để xác định các nút mạng có thể bị lây nhiễm bởi handlers.
- **Vô hiệu hóa Botnet handlers** – số lượng DDoS handler được triển khai trong mạng ít hơn nhiều so với số lượng agents. Việc vô hiệu hóa một số handler có thể khiến nhiều agent trở nên vô dụng từ đó ngăn chặn các cuộc tấn DDoS.
- **Địa chỉ nguồn giả mạo** – thường thì địa chỉ nguồn giả mạo của các gói DDoS sẽ không đại diện cho địa chỉ nguồn hợp lệ của mạng con xác định.



Prevent Potential Attack

Egress Filtering

- Egress filtering quét IP hearder ra khỏi mạng và đảm bảo rằng lưu lượng truy cập độc hại hoặc trái phép sẽ không bao giờ ra khỏi mạng nội bộ.

Ingress Filtering

- Ingress filtering (IF) ngăn chặn việc giả mạo địa chỉ nguồn, bảo vệ mạng khỏi các cuộc tấn công flood bắt nguồn từ các địa chỉ IP hợp lệ và cho phép «originator» tìm nguồn gốc thực sự của nó.

TCP Intercept

- Tính năng chặn TCP trong router bảo vệ TCP server khỏi tấn công SYN-flood thông qua việc xác thực các yêu cầu kết nối TCP.

Rate Limit

- «Rate limiting» kiểm soát tốc độ lưu lượng đi hoặc đến của NIC
- Làm giảm lưu lượng các truy cập đến có khối lượng lớn.

Deflect Attacks

- Sử dụng hệ thống mồi nhử như Honeypot để thu thập thông tin về attacker, các kỹ thuật và công cụ được sử dụng. Có 2 loại honeypots cơ bản:
  - Low-interaction honeypots (honeynet)
  - High-interaction honeypots
- Sử dụng phương pháp "defense-in-depth" cùng với một số IPS đặt tại các điểm khác nhau trong mạng để sớm phát hiện các lưu lượng DoS nghi ngờ.

Mitigate Attacks

Load Balancing

- Tăng băng thông trên các kết nối trọng yếu để hấp thụ lưu lượng bổ sung do tấn công tạo ra.
- «Nhân bản» các servers để đảm bảo dự phòng.
- Thực hiện cân bằng tải trên mỗi máy chủ trong kiến trúc nhiều máy chủ.

Throttling

- Thiết lập router với mức lưu lượng đến an toàn cho server có thể xử lý.
- Phương pháp này lọc lưu lượng người dùng hợp pháp khỏi lưu lượng tấn công DDoS giả mạo.

Drop Request

- Servers, routers sẽ «drop» các gói khi tải tăng lên.
- Hệ thống khiến «requester» từ bỏ yêu cầu bằng cách bắt nó giải một câu đố khó đòi hỏi nhiều bộ nhớ hoặc khả năng tính toán trước khi tiếp tục yêu cầu.

Post-Attack Forensics

Traffic Pattern Analysis	❑ Phát triển các kỹ thuật lọc mới để ngăn chặn lưu lượng tấn công (đi vào hoặc rời khỏi mạng). ❑ Giúp cập nhật việc thực hiện cân bằng tải, điều chỉnh các biện pháp phòng chống để nâng cao hiệu quả và khả năng bảo vệ.
Packet Traceback	❑ Packet Traceback tương tự như "reverse engineering". ❑ Nó giúp xác định nguồn gốc thực sự của tấn công và thực hiện các bước cần thiết để ngăn chặn tấn công trong tương lai.
Event Log Analysis	❑ Giúp xác định nguồn gốc của lưu lượng DoS. ❑ Cho phép quản trị viên xác định loại tấn công DoS/DDoS được sử dụng.

Techniques to Defend against Botnets (1/2)

RFC 3704 Filtering

- RFC 3704 Filtering hạn chế tác động của các cuộc tấn công bằng cách từ chối lưu lượng truy cập với các địa chỉ giả mạo.
- Bất kỳ lưu lượng truy cập nào đến từ các địa chỉ ip không sử dụng hoặc dành riêng đều là không có thật và cần được lọc tại ISP trước khi nó đi vào liên kết internet.

IPS Source IP Reputation Filtering

- Dịch vụ uy tín giúp xác định xem IP hoặc dịch vụ có phải là nguồn đe dọa hay không.
- Các thiết bị như IPS thường xuyên cập nhật cơ sở dữ liệu của mình với các mối đe dọa đã biết như mạng botnet, malware v.v. và giúp lọc lưu lượng DoS.

Techniques to Defend against Botnets (2/2)

Black Hole Filtering

- «Blackhole» đề cập đến các nút mạng nơi lưu lượng đến bị loại bỏ hoặc bị giảm mà không thông báo cho nguồn rằng dữ liệu không đến được người nhận dự kiến.
- «Blackhole filtering» đề cập đến việc loại bỏ các gói ở mức định tuyến.

DDoS Prevention Offerings from ISP or DDoS Service

- Phương pháp này hiệu quả trong việc ngăn chặn giả mạo IP ở mức ISP - ISP sẽ xóa hoặc làm sạch lưu lượng truy cập trước khi cho phép nó truy cập vào liên kết internet của người dùng.
- Một số bên thứ ba cung cấp dịch vụ ngăn chặn ddos trên đám mây.

Additional DoS/DDoS Countermeasures (1/2)

- Sử dụng các cơ chế mã hóa mạnh như WPA2 và AES 256 cho các mạng băng thông rộng để chống lại việc nghe trộm.
- Đảm bảo rằng OS, kernel, phần mềm, giao thức được cập nhật bản phát hành mới nhất. Dò quét hệ thống kỹ lưỡng để phát hiện bất kỳ hành vi bất thường nào.
- Vô hiệu hóa các dịch vụ không sử dụng và không an toàn.
- Chặn tất cả các gói đến có nguồn gốc từ các cổng dịch vụ để chặn lưu lượng ánh xạ từ các máy chủ khác.
- Ngăn chặn việc truyền các gói có địa chỉ giả mạo ở cấp ISP.

Additional DoS/DDoS Countermeasures (2/2)

- Triển khai công nghệ vô tuyến nhận thức (cognitive radio) trong tầng vật lý để xử lý các cuộc tấn công gây nhiễu.
- Cấu hình tường lửa để từ chối truy cập lưu lượng ICMP bên ngoài.
- Phòng chống DoS/DDoS tại mức ISP, chặn lưu lượng tấn công tại gateway.
- Thực hiện mô phỏng tấn công DoS và các biện pháp ứng phó.
- Sử dụng dịch vụ phòng chống DoS của bên thứ 3.

Enabling TCP Intercept on Cisco IOS

- Để bật tính năng "TCP Intercept" trên CISCO IOScó thể sử dụng các lệnh sau trong chế độ "global configuration".

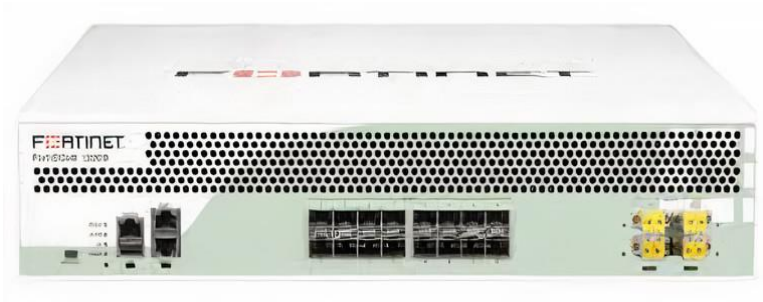
Step	Command	Purpose
1	access-list access-list-number{deny|permit} tcp any destination destination-wildcard	Define an IP extended access list
2	Ip tcp intercept list access-list-number	Enable TCP intercept

- "TCP intercept" có thể hoạt động ở chế độ "active intercept" hoặc chế độ "passive watch". Mặc định là chế độ "active intercept".
- Thiết lập "TCP intercept mode" trong chế độ "global configuration".

Command	Purpose
ip tcp intercept mode {intercept|watch}	Set the TCP intercept

Advanced DDoS Protection Appliances

FortiDDoS-1200B



DDoS Protector

Cisco Guard TX 5650

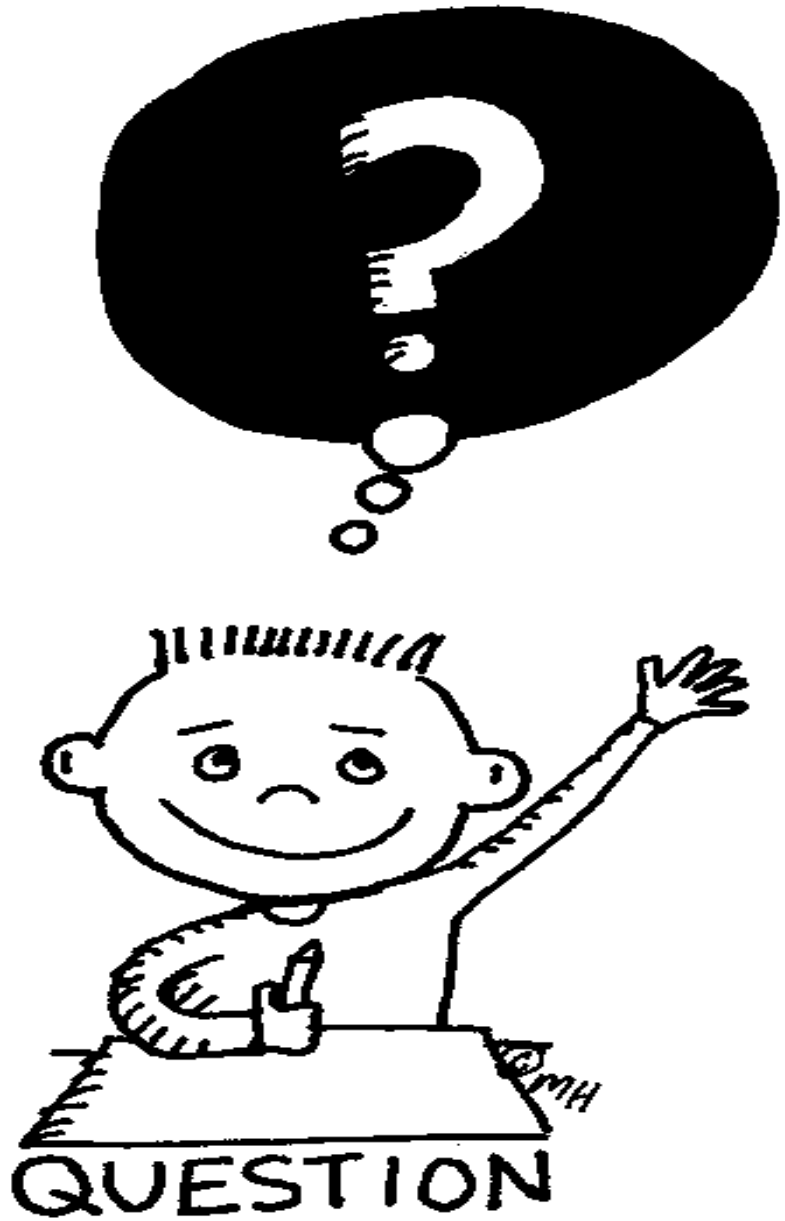
A10 Thunder TPS

DoS/DDoS Protection Tools & Service

- Anti DDoS Guardian (http://www.beethink.com)
- DDoS-GUARD (http://ddos-guard.net)
- Cloudflare(http://www.cloudflare.com)
- DOSarrest's DDoS protection service (http://www.dosarrest.com)
- DefensePro (http://www.radware.com)
- DDoS Protection (https://www.imperva.com)
- Kaspersky DDoS Protection Tool
- Nexusguard
- Coreto DDoS Protection
- Stormwall PRO

TOPIC

- Phân tích một số vụ tấn công từ chối dịch vụ nổi tiếng


QUESTION