CÔNG AN TỈNH HẢI DƯƠNG
CÔNG AN HUYỆN THANH MIỆN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 705/TB-CATM

Thanh Miện, ngày 27 tháng 4 năm 2023

V/v cảnh báo nguy cơ tấn công từ chối dịch vụ với mạng máy tính

Kính gửi: - Đồng chí Trưởng các ban, ngành của huyện;
- Đồng chí Chủ tịch UBND các xã, thị trấn;
- Các doanh nghiệp, ngân hàng trên địa bàn huyện.

Qua trao đổi với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh Hải Dương, căn cứ kết quả nắm tình hình, thực hiện đảm bảo an ninh, an toàn thông tin mạng, Công an huyện thông tin, cảnh báo nguy cơ mất an toàn an ninh mạng về nguy cơ tấn công từ chối dịch vụ với mạng máy tính (DoS và DDoS) như sau:

1. Tấn công từ chối dịch vụ DoS (Denial of Service - từ chối dịch vụ) là việc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó. Bằng cách gửi nhiều yêu cầu hoặc thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu, DoS khiến người dùng (gồm nhân viên, thành viên, chủ tài khoản) không thể truy cập dịch vụ, tài nguyên mong đợi. Tấn công DoS thường nhắm tới máy chủ web của các tổ chức như ngân hàng, doanh nghiệp, các trang báo, mạng xã hội... thậm chí có thể sử dụng thư rác để thực hiện các tấn công tương tự với tài khoản email cá nhân. Tài khoản email của cơ quan hay dùng dịch vụ miễn phí như Gmail vẫn bị giới hạn số lượng dữ liệu trong tài khoản. Bằng cách gửi nhiều email đến tài khoản email cá nhân/cơ quan, DoS có thể làm đầy hòm thư đến và ngăn chặn nhận các email khác.

Tấn công DDoS (Distributed Denial of Service - từ chối dịch vụ phân tán) là một dạng tấn công server chứa website, gây cạn kiệt tài nguyên hệ thống máy chủ, ngập lưu lượng băng thông internet và làm gián đoạn kết nối người dùng. Khi DDoS có thể sử dụng máy tính của một cá nhân để tấn công vào các máy tính khác. Bằng cách lợi dụng những lỗ hổng về bảo mật cũng như sự thiếu hiểu biết, DDoS có thể chiếm quyền điều khiển máy tính cá nhân và sử dụng máy tính này để gửi số lượng lớn dữ liệu đến một website hoặc gửi thư rác đến địa chỉ email nào đó. Đây là kiểu tấn công phân tán vì sử dụng nhiều máy tính, bao gồm cả máy tính cá nhân để thực hiện tấn công DoS.

DDoS ngày càng mạnh và tinh vi với ba loại tấn công: Volume-based (Sử dụng lưu lượng truy cập cao để làm tràn ngập băng thông mạng); Protocol (Tập trung vào việc khai thác các tài nguyên máy chủ); Application (Tập trung vào các ứng dụng web - đây được xem là loại tấn công tinh vi và nghiêm trọng nhất).

2. Các cuộc tấn công DoS, DDoS được thực hiện với mạng các máy kết nối Internet. Biểu hiện rõ nhất của cuộc tấn công từ chối dịch vụ là một trang

web hoặc dịch vụ đột nhiên trở nên chậm chạp hoặc không khả dụng. Một số biểu hiện khác:

+ Thực thi mạng chậm một cách không bình thường (mở file hay truy cập website).

+ Không vào được website vẫn thường xem.

+ Không thể truy cập đến bất kỳ một website nào.

+ Số lượng thư rác tăng một cách đột biến trong tài khoản.

+ Lưu lượng truy cập đáng ngờ bắt nguồn từ một địa chỉ IP hoặc dải IP/một lượng lớn lưu lượng truy cập từ những người dùng chia sẻ một profile hành vi, chẳng hạn như loại thiết bị, vị trí địa lý hoặc phiên bản trình duyệt web.

+ Các mẫu lưu lượng truy cập kỳ lạ, ví dụ như tăng đột biến vào các giờ cụ thể trong ngày hoặc có vẻ không tự nhiên.

3. Các kiểu tấn công từ chối dịch vụ phổ biến hiện nay:

SYN Flood: khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều. Máy chủ sẽ nhận được một thông điệp đồng bộ (SYN) để bắt đầu "bắt tay". Máy chủ nhận tin nhắn bằng cách gửi cờ báo nhận (ACK) tới máy lưu trữ ban đầu, sau đó đóng kết nối. Tuy nhiên, trong một SYN Flood, tin nhắn giả mạo được gửi đi và kết nối không đóng, dẫn đến dịch vụ sập.

UDP Flood: nhắm đến các cổng ngẫu nhiên trên máy tính hoặc mạng với các gói tin UDP. Máy chủ kiểm tra ứng dụng tại các cổng đó nhưng không tìm thấy ứng dụng nào.

HTTP Flood: gần giống như các yêu cầu GET hoặc POST hợp pháp được khai thác bởi một hacker, sử dụng ít băng thông hơn các loại tấn công khác nhưng nó có thể buộc máy chủ sử dụng các nguồn lực tối đa.

Ping of Death: điều khiển các giao thức IP bằng cách gửi những đoạn mã độc đến một hệ thống.

Smurf Attack: khai thác giao thức Internet (IP) và ICMP (Internet Control Message Protocol) sử dụng một chương trình phần mềm độc hại gọi là smurf. Nó giả mạo một địa chỉ IP và sử dụng ICMP, sau đó ping các địa chỉ IP trên một mạng nhất định.

Fraggle Attack: sử dụng một lượng lớn lưu lượng UDP vào mạng phát sóng của router. Nó giống như một cuộc tấn công Smurf, sử dụng UDP nhiều hơn là ICMP.

Slowloris: sử dụng nguồn lực tối thiểu trong một cuộc tấn công và các mục tiêu trên máy chủ web. Khi đã kết nối với mục tiêu mong muốn, Slowloris giữ liên kết đó mở càng lâu càng tốt với HTTP tràn ngập.

Application Level Attacks: khai thác lỗ hổng trong các ứng dụng. Mục tiêu của loại tấn công này không phải là toàn bộ máy chủ, mà là các ứng dụng với những điểm yếu được biết đến.

NTP Amplification: khai thác các máy chủ NTP (Network Time Protocol), một giao thức được sử dụng để đồng bộ thời gian mạng, làm tràn ngập lưu lượng UDP. Đây là reflection attack bị khuếch đại. Trong reflection attack bất kỳ nào đều sẽ có phản hồi từ máy chủ đến IP giả mạo, khi bị khuếch đại, thì phản hồi từ máy chủ sẽ không còn tương xứng với yêu cầu ban đầu. Vì

sử dụng băng thông lớn khi bị DDoS nên loại tấn công này có tính phá hoại và volumne cao.

Advanced Persistent DoS (APDoS): sử dụng nhiều kiểu tấn công được đề cập trước đó (HTTP Flood, SYN Flood...) và thường nhắm tấn công theo kiểu gửi hàng triệu yêu cầu/giây. Các cuộc tấn công của APDoS có thể kéo dài hàng tuần, phụ thuộc vào khả năng của hacker để chuyển đổi các chiến thuật bất cứ lúc nào và tạo ra sự đa dạng để tránh các bảo vệ an ninh.

Zero-day DDoS Attacks: phương pháp tấn công DDoS mới, khai thác các lỗ hổng chưa được vá.

HTTP GET: Kiểu tấn công này sẽ nhắm vào lớp thứ 7 trong mô hình OSI. Đây là lớp có lưu lượng mạng cao nhất, thay vì hướng vào lớp thứ 3 thường được chọn làm mục tiêu trong các cuộc tấn công Bulk Volumetric. HTTP GET khai thác quy trình của một trình duyệt web hoặc ứng dụng HTTP nào đó và yêu cầu một ứng dụng hoặc máy chủ cho mỗi yêu cầu HTTP, đó là GET hoặc POST.

4. Các cuộc tấn công từ chối dịch vụ ngày càng phổ biến và thường diễn ra âm thầm, song cũng nhanh chóng gây hại với mạng máy tính nếu không được ngăn chặn, xử lý kịp thời. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin các cơ quan, đơn vị, doanh nghiệp, đồng thời chủ động đảm bảo an ninh mạng, Công an huyện đề nghị các cơ quan, ban ngành, doanh nghiệp, UBND các xã, thị trấn trên địa bàn huyện chủ động thực hiện:

+ Cài đặt và duy trì phần mềm chống virus. Cài đặt tường lửa và cấu hình nó để giới hạn lưu lượng đến và đi từ máy tính cá nhân.

+ Làm theo các hướng dẫn thực hành an toàn về phân phối địa chỉ email. Dùng các bộ lọc email để quản lý lưu lượng không mong muốn.

+ Quét mạng thường xuyên và theo dõi lưu lượng với các cảnh báo. Nếu nhận thấy những vấn đề xảy ra trên máy tính, liên hệ với nhà cung cấp dịch vụ (ISP).

+ Kiểm tra và nâng cao bảo mật của trang web, fanpage, tài khoản quản trị viên, người kiểm duyệt có liên quan.

+ Làm sạch dữ liệu, thường xuyên bảo trì hệ thống cung cấp dịch vụ mạng internet, máy tính và các thiết bị liên quan (máy quét, máy in...) để hoạt động an toàn, hiệu quả.

Vậy Công an huyện thông báo để các đồng chí nắm được, chủ động công tác bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị./.

Nơi nhận:
- Như trên;
- Đ/c Bí thư Huyện ủy;
- Đ/c Chủ tịch UBND huyện;
- Đ/c Giám đốc CAT (qua PA05); (Để báo cáo)
- Lưu: Đội AN.

TRƯỞNG CÔNG AN HUYỆN

CÔNG AN TỈNH HẢI DƯƠNG
CÔNG AN HUYỆN THANH MIỆN

Thượng tá Vũ Khắc Hội