Y Tá Đen - Kỹ thuật DDoS giúp cho một laptop bình thường cũng có thể hạ gục cả hệ thống máy chủ

Ngay cả khi các máy chủ đó được trang bị những thiết bị tường lửa nổi tiếng, chúng vẫn có thể bị đánh gục nếu kẻ tấn công khai thác kỹ thuật này.

Nghe có vẻ khó tin, nhưng thay vì một mạng botnet khổng lồ, bạn chỉ cần một chiếc laptop với một đường kết nối Internet để phát động cuộc tấn công**DDoS** mạnh mẽ, hạ gục các máy chủ Internet quan trọng và các tường lửa hiện đại.

Các nhà nghiên cứu tại Trung tâm Điều hành Bảo mật TDC đã khám phá ra một kỹ thuật tấn công mới, cho phép những kẻ tấn công đơn lẻ với nguồn lực hạn chế (trong trường hợp này, là một laptop với một đường mạng băng thông có băng thông ít nhất 15 Mbps) có thể **hạ gục các máy chủ** cỡ lớn.

Được mệnh danh là **kỹ thuật tấn công BlackNurse - Y Tá Đen** hay **tấn công tốc độ thấp "*Ping of Death*"**, kỹ thuật này có thể được sử dụng để phát động hàng loạt cuộc tấn công từ chối dịch vụ DoS khối lượng thấp bằng cách gửi các gói tin ICMP hay các "ping" để làm ngập những bộ xử lý trên máy chủ.

Ngay cả những máy chủ được bảo vệ bằng **tường lửa từ Cisco**, **Palo Alto Networks**, hay các công ty khác cũng bị ảnh hưởng bởi kỹ thuật tấn công này.

ICMP (Internet Control Message Protocol) là giao thức được các router và các thiết bị mạng lưới khác sử dụng để gửi đi và nhận lại các thông báo lỗi.

Ping of Death là kỹ thuật tấn công làm quá tải hệ thống mạng bằng cách gửi các gói tin ICMP có kích thước vượt quá 65.536 byte đến mục tiêu. Do kích thước này lớn hơn kích thước cho phép của các gói tin IP nên nó sẽ được chia nhỏ ra rồi gửi từng phần đến máy đích. Khi đến mục tiêu, nó sẽ được ráp lại thành gói tin hoàn chỉnh, do có kích thước quá mức cho phép, nó sẽ gây ra tràn bộ nhớ đệm và bị treo.

Theo một báo cáo kỹ thuật được công bố trong tuần này, kỹ thuật tấn công BlackNurse còn được biết đến dưới một cái tên truyền thống hơn: "*tấn công gây lụt ping*" và nó dựa trên các truy vấn ICMP Type 3 (hay lỗi Đích tới Không thể truy cập – Destination Unreachable) Code 3 (lỗi Cổng Không thể truy cập – Port Unreachable).

Các truy vấn này là những gói tin trả lời, thông thường sẽ trở lại nguồn ping khi cổng đích đến của mục tiêu không thể truy cập – hay **Unreachable**.

1. Dưới đây là cách kỹ thuật tấn công BlackNurse hoạt động:

Bằng cách gửi đi một gói tin **ICMP Type 3** với một mã số là 3, một hacker có thể gây ra tình trạng từ chối dịch vụ (DoS) bằng cách làm quá tải các CPU trên một số loại tường lửa nhất định của máy chủ, cho dù chất lượng của đường Internet thế nào đi nữa.

Khối lượng truy cập bằng kỹ thuật **BlackNurse** rất nhỏ, chỉ từ 15 Mbps cho đến 18 Mbps (hay khoảng từ 40.000 đến 50.000 gói tin mỗi giây), đặc biệt khi so sánh với cuộc tấn công DDoS kỷ lục 1 Tbps nhắm vào nhà cung cấp dịch vụ Internet của Pháp OVH trong tháng Chín.

Trong khi đó, TDC cũng cho biết rằng khối lượng khổng lồ này không phải vấn đề quan trọng khi chỉ cần duy trì một dòng ổn định các gói tin ICMP từ 40K đến 50K đến được thiết bị mạng của nạn nhân là có thể phá hủy thiết bị mục tiêu.

Vậy tin tốt ở đây là gì? Các nhà nghiên cứu cho biết: "*Khi cuộc tấn công diễn ra, người dùng trong mạng nội bộ LAN sẽ không thể gửi hay nhận các truy cập đi và đến Internet nữa. Tất cả tường lửa mà chúng tôi đã thấy đều phục hồi sau khi cuộc tấn công dừng lại*."

Tuy vậy, điều này có nghĩa là, kỹ thuật tấn công DoS khối lượng thấp này vẫn rất hiệu quả bởi vì nó không chỉ gây lụt tường lửa bằng các truy cập, mà còn buộc các CPU phải tải với mức độ cao, thậm chí hạ gục các máy chủ offline nếu cuộc tấn công có đủ công suất mạng.

Các nhà nghiên cứu cho rằng không nên nhầm lẫn **BlackNurse** với các cuộc tấn công gây lụt ping dựa trên các gói tin ICMP Type 8 Code 0 (hay những gói tin ping thường xuyên). Các nhà nghiên cứu giải thích:

"*Kỹ thuật tấn công BlackNurse thu hút sự chú ý của chúng tôi bởi vì trong cuộc thử nghiệm giải pháp chống DDoS, ngay cả khi tốc độ truy cập và khối lượng các gói tin mỗi giây ở mức độ rất thấp, cuộc tấn công này cũng có thể làm dừng mọi hoạt động của khách hàng chúng tôi*."

"*Thậm chí, kỹ thuật tấn công này cũng có thể áp dụng cho các doanh nghiệp được trang bị tường lửa và có đường kết nối Internet lớn. Chúng tôi hy vọng*

rằng các thiết bị tường lửa chuyên nghiệp sẽ có thể xử lý được các cuộc tấn công này."

2. Các thiết bị bị ảnh hưởng

Kỹ thuật tấn công BlackNurse có hiệu quả với các sản phẩm sau:

- Thiết bị tường lửa Cisco ASA 5506, 5515, 5525 (ở các cài đặt mặc định).
- Thiết bị tường lửa Cisco ASA 5550 (đời cũ) và 5515-X (thế hệ mới nhất).
- Cisco Router 897 (có thể bị giảm nhẹ).
- SonicWall (cấu hình sai có thể bị thay đổi và giảm nhẹ).
- Một số thiết bị chưa xác định từ Palo Alto.
- Router Zyxel NWA3560-N (tấn công không dây từ mạng LAN nội bộ).
- Thiết bị tường lửa Zyxel Zywall USG50.

3. Làm thế nào để giảm nhẹ cuộc tấn công BlackNurse?

Vẫn còn tin tốt cho bạn – có một số cách có thể đánh trả lại các cuộc tấn công BlackNurse.

TDC đề nghị một số biện pháp giảm nhẹ và các quy tắc **IDS SNORT** (hệ thống phát hiện xâm nhập theo mã nguồn mở SNORT) có thể sử dụng để phát hiện các cuộc tấn công BlackNurse. Hơn nữa, các code PoC (proof-of-concept: mã bằng chứng của khái niệm) đã được các kỹ sư OVH đăng tải lên GitHub, cũng có thể sử dụng để thử nghiệm thiết bị của các nhà quản trị mạng trong việc chống lại BlackNurse.

Để giảm nhẹ các cuộc tấn công BlackNurse vào tường lửa và các thiết bị khác, TDC khuyến cáo người dùng nên **lập ra một danh sách các nguồn đáng tin cậy, được phép gửi và nhận gói tin ICMP**. Tuy nhiên, cách tốt nhất để giảm nhẹ cuộc tấn công chỉ đơn giản là vô hiệu hóa gói tin ICMP Type 3 Code 3 trên giao diện WAN.

Công ty Palo Alto Networks cũng phát hành một tuyên bố, cho biết các thiết bị của mình chỉ bị ảnh hưởng theo "*các kịch bản rất cụ thể, không phải trong thiết lập mặc định và trái với các thông lệ thường thấy*." Công ty cũng đã liệt kê một số khuyến cáo cho khách hàng của mình.

Trong khi đó, Cisco cho biết họ không cho rằng hành vi trong báo cáo là một vấn đề an ninh, mà cảnh báo rằng:

"*Chúng tôi khuyến cáo mọi người thiết lập giấy phép cho các gói tin không thể truy cập ICMP Type 3. Từ chối các thông điệp không thể truy cập ICMP giúp vô hiệu hóa giao thức Path MTU Discovery cho gói tin ICMP. Những việc này có thể ngăn chặn IPSec (Internet Protocol Security: tập hợp các giao thức để bảo mật cho quá trình truyền tin) và truy cập theo giao thức PPTP (Point-To-Point Tunneling Protocol: Là giao thức được dùng để truyền dữ liệu giữa các mạng riêng ảo VPN).*"

Hơn nữa, nhà cung cấp phần mềm độc lập NETRESEC cũng công bố một bản phân tích chi tiết về BlackNurse với tựa đề: "*Kỹ thuật tấn công gây ngập lụt từ những năm 90 đã quay trở lại*." Bên cạnh các cảnh báo trên, Viện Sans cũng thông báo một bản ghi nhớ ngắn về cuộc tấn công của BlackNurse, thảo luận về cuộc tấn công và những gì người dùng nên làm để giảm nhẹ nó