Nguồn
APT Profile: Who is Lazarus Group? - SOCRadar® Cyber Intelligence Inc.
Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang (talosintelligence.com)

lazarus: Lazarus Group, hay còn gọi là APT38, được cho là có trụ sở tại Triều Tiên

[Cập nhật] Ngày 12 tháng 12 năm 2023: Xem tiêu đề phụ: "Lazarus sử dụng Log4Shell trong chiến dịch Blacksmith, triển khai phần mềm độc hại mới: NineRAT, DLRAT và BottomLoader".

campaign: Operation Blacksmith

hợp tác: nhóm Onyx Sleet (PLUTIONIUM)

ảnh hưởng: phạm vi toàn cầu, mục tiêu cụ thể: manufacturing, agricultural and physical security companies.

Lỗ hổng: khai thác lỗ hổng Log4Shell RCE (CVE-2021-44228) / Log4j vulnerability discovered in 2021.

tấn công mục tiêu: Máy chủ VMWare Horizon bị lộ ra ngoài, sử dụng phiên bản thư viện ghi nhật ký Log4j dễ bị tấn công.

Malware: ba phần mềm độc hại mới được viết bằng DLang: trojan truy cập từ xa NineRAT và DLRAT và một trình tải xuống phần mềm độc hại có tên BottomLoader

NineRAT: sử dụng API Telegram để giao tiếp C2, tạo điều kiện thuận lợi cho việc truyền tệp và tránh bị phát hiện
command NineRAT dùng:

/setmtoken	Set a token value.
/setbtoken	Set a new Bot token.
/setinterval	Set time interval between malware polls to the Telegram channel.
/setsleep	Set a time period for which the malware should sleep/lie dormant.
/upgrade	Upgrade to a new version of the implant.
/exit	Exit execution of the malware.
/uninstall	Uninstall self from the endpoint.
/sendfile	Send a file to the C2 server from the infected endpoint.

DLRAT: là một RAT trình tải xuống mà Lazarus có thể sử dụng để triển khai phần mềm độc hại bổ sung và truy xuất các lệnh từ C2. Khi xâm nhập vào một thiết bị, DLRAT thực hiện các lệnh được mã hóa cứng để trinh sát, thu thập thông tin hệ thống và trích xuất nó đến máy chủ C2.

command NineRAT dùng

deleteme	Delete itself from the system using a BAT file.
download	Download files from a specified remote location.
rename	Rename files on the system.
iamsleep	Instructs the implant to go to sleep for a specified amount of time.
upload	Upload files to C2.
showurls	Empty command (Not implemented yet).

Bottomloader: BottomLoader là một trình tải xuống phần mềm độc hại truy xuất và thực thi các tải trọng giai đoạn tiếp theo từ một máy chủ từ xa, như HazyLoad. Các nhà nghiên cứu lưu ý rằng nó có thể tải xuống tải trọng từ một URL từ xa được mã hóa cứng và tải tệp lên C2 bằng các lệnh PowerShell. Ngoài ra, BottomLoader có thể thiết lập sự bền bỉ cho các phiên bản mới hơn hoặc tải trọng mới bằng cách sửa đổi thư mục Khởi động.

summary campaign: Operation Blacksmith
Lazarus bắt đầu truy cập bằng cách khai thác lỗ hổng Log4j được phát hiện vào năm 2021 ,mục tiêu là các máy chủ VMWare Horizon public, sử dụng phiên bản thư viện ghi nhật ký Log4j dễ bị tấn công.

Sau khi khai thác lỗ hổng, Lazarus thiết lập quyền truy cập liên tục bằng công cụ proxy HazyLoad, chạy các lệnh trinh sát, tạo tài khoản người dùng đặc quyền quản trị và triển khai các công cụ đánh cắp thông tin xác thực như ProcDump và MimiKatz. Microsoft trước đó đã xác định HazyLoad trong các cuộc tấn công Lazarus khai thác lỗ hổng bảo mật nghiêm trọng trong JetBrains TeamCity (CVE-2023-42793). HazyLoad được tải xuống và thực thi bởi phần mềm độc hại loader được gọi là BottomLoader.

NineRAT được phóng trong giai đoạn thứ hai, ban đầu được Lazarus quan sát thấy sử dụng vào đầu tháng 3/2023. Sau khi kích hoạt, NineRAT nhận lệnh thông qua kênh C2 dựa trên Telegram, cho phép lấy dấu vân tay của các hệ thống bị nhiễm. Các nhà nghiên cứu cho rằng việc lấy lại dấu vân tay chỉ ra rằng dữ liệu do Lazarus thu thập thông qua NineRAT có thể được chia sẻ với các nhóm APT khác, nằm trong một kho lưu trữ khác với dữ liệu dấu vân tay ban đầu được thu thập trong quá trình truy cập ban đầu của Lazarus.