Một tin tặc bị buộc tội âm mưu phát triển và triển khai phần mềm độc hại khai thác hàng chục nghìn tường lửa trên toàn thế giới

Tuesday, December 10, 2024

Bản dịch tóm tắt:

Một tòa án liên bang ở Hammond, Indiana (Mỹ), đã công bố cáo trạng buộc tội Guan Tianfeng (tên Hán Việt là "Quan Thiên Phong") vì liên quan đến âm mưu tấn công bừa bãi vào các thiết bị tường lửa trên toàn thế giới.

Năm 2020, Guan đã phát hiện và khai thác một **lỗ hổng** chưa từng được biết đến trước đây **(lỗ hổng "zero-day"**) trong một số thiết bị tường lửa ('firewall device') do hãng Sophos Ltd. (có trụ sở tại Anh) bán cho khách hàng *(Sophos là một công ty CNTT phát triển và tiếp thị các sản phẩm an ninh mạng).*

Phần mềm độc hại (mã độc) khai thác **lỗ hổng** do Guan phát hiện được thiết kế để đánh cắp thông tin từ các máy tính bị nhiễm mã độc, mã hóa 'files' trên đó nếu nạn nhân cố gắng khắc phục sự cố nhiễm mã độc. Lỗ hổng zero-day Guan Tianfeng và những kẻ đồng phạm đã tìm thấy và khai thác các tường lửa bị ảnh hưởng do các doanh nghiệp trên khắp Hoa Kỳ sở hữu. Tổng cộng, Guan và những kẻ đồng phạm đã lây nhiễm mã độc cho khoảng 81.000 thiết bị tường lửa trên toàn thế giới, gây nguy hiểm cho các thiết bị này và làm suy yếu an ninh mạng toàn cầu.

Guan và những kẻ đồng phạm đã khai thác **lỗ hổng** trong hàng chục nghìn thiết bị an ninh mạng, lây nhiễm phần mềm độc hại được thiết kế để đánh cắp thông tin từ nạn nhân trên toàn thế giới. Hành động khai thác lỗ hổng zero-day của những kẻ tấn công mạng này đã gây ra **mối đe dọa** đối với an ninh mạng toàn cầu.

Lỗ hổng zero-day này sau đó được chỉ định là CVE 2020-12271.

(…)

Cập nhật ngày 6 tháng 2 năm 2025

Xem trang https://www.justice.gov/archives/opa/pr/china-based-hacker-charged-conspiring-develop-and-deploy-malware-exploited-tens-thousands