

UBND TỈNH LAI CHÂU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-BCVTCNTT
V/v Cảnh báo phát hiện mã độc
Trojan Redline Stealer gây ảnh hưởng
trên các hệ thống thông tin.

Lai Châu, ngày tháng năm 2024

Kính gửi:

- Các Sở, Ban, Ngành tỉnh;
- UBND các huyện, thành phố.

Qua công tác giám sát an toàn không gian mạng quốc gia, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin - Bộ Thông tin và Truyền thông, ghi nhận thông tin liên quan đến mã độc Trojan Redline Stealer được sử dụng để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức.

Một biến thể mới của mã độc Trojan Redline Stealer đã được phát hiện trên không gian mạng, mã độc này triển khai các bytecode Lua để thực hiện các hành vi độc hại. Dữ liệu cho thấy mã độc đang rất phổ biến khi nó lây nhiễm trải dài Bắc Mỹ, Nam Mỹ, Châu Âu, Châu Á và Úc. Để đảm bảo an toàn cho hệ thống thông tin, các cơ quan, tổ chức cần thực hiện kiểm tra, rà soát và chuẩn bị các phương án xử lý kịp thời khi phát hiện có dấu hiệu bị tấn công.

(Thông tin chi tiết xem tại Phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý Đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ hãng nhằm thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát

hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin để được hỗ trợ: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Phòng Bru chính - Viễn thông - Công nghệ thông tin, số điện thoại: 02133.798.798.

Trên đây là cảnh báo cảnh báo phát hiện mã độc Trojan Redline Stealer gây ảnh hưởng trên các hệ thống thông tin, Sở Thông tin và Truyền thông kính đề nghị Quý cơ quan quan tâm thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT, BCVTCNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Trần Văn Sáu

Phụ lục
THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC
(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2024 của Sở
Thông tin và Truyền thông)

1. Thông tin chi tiết về mã độc Trojan Redline Stealer

RedLine Stealer là mã độc xuất hiện lần đầu tiên vào khoảng tháng 3 năm 2020, mã độc này có khả năng trích xuất thông tin đăng nhập từ nhiều nguồn khác nhau, bao gồm trình duyệt web, ứng dụng FTP, email, Steam, ứng dụng nhắn tin và VPN.

Một biến thể mới của mã độc Trojan Redline Stealer đã được phát hiện trên không gian mạng, mã độc này triển khai các bytecode Lua để thực hiện các hành vi độc hại. Dữ liệu cho thấy mã độc đang rất phổ biến khi nó lây nhiễm trải dài Bắc Mỹ, Nam Mỹ, Châu Âu, Châu Á và Úc.

Các đơn vị có thể tải xuống các mã dấu hiệu của sự xâm nhập (IOC) tại <https://alert.khonggianmang.vn/>

Dưới đây là một số dấu hiệu của sự xâm nhập được ghi nhận:

Cheat.Lab.2.7.2.zip	5e37b3289054d5e774c02a6ec491 5a60156d715f3a02aaceb7256cc3e bdc6610
Cheat.Lab.2.7.2.zip	https://github.com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
lua51.dll	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749 d7631f2912bcb640439997
readme.txt	751f97824cd211ae710655e60a26885cd79974f0f 0a5e4e582e3b635492b4cad
compiler.exe	dfbf23697cfd9d35f263af7a455351480920a95bfc 642f3254ee8452ce20655a

Redline C2	213[.]248[.]43[.]158
Trojanised Git Repo	hxxps://github.com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip

2. Tài liệu tham khảo

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/>