UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 786 /STTTT-TTGSĐH
V/v cảnh báo phát hiện mã độc trojan Radline Stealer gây ảnh hưởng trên các hệ thống thông tin.

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

Tây Ninh, ngày26 tháng 04 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 722/CATTT-NCSC, ngày 24/4/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo phát hiện mã độc trojan Radline Stealer gây ảnh hưởng trên các hệ thống thông tin. *(Thông tin chi tiết phụ lục kèm theo).*

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông khuyến nghị các Đơn vị, địa phương thực hiện các công việc cụ thể như sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc trojan Radline Stealer. 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.

Thông tin liên hệ Ông Đào Quang Phúc - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0937.117.128./.

Trân trọng!

Nơi nhận:
- Như trên;
- BGĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

Phụ lục

THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

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 IOC tại https://alert.khonggianmang.vn/

Dưới đây là một số IoC được ghi nhận

Cheat.Lab.2.7.2.zip	5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610
Cheat.Lab.2.7.2.zip	https[:]//github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
lua51.dll	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749d7631f2912bcb640439997
readme.txt	751f97824cd211ae710655e60a26885cd79974f0f0a5e4e582e3b635492b4cad
compiler.exe	dfbf23697cfd9d35f263af7a455351480920a95bfc642f3254ee8452ce20655a
Redline C2	213[.]248[.]43[.]58
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/