| | |
|---|---|
| BỘ THÔNG TIN TRUYỀN THÔNG<br>**CỤC AN TOÀN THÔNG TIN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 722 /CATTT-NCSC<br>V/v cảnh báo phát hiện mã độc trojan Redline Stealer gây ảnh hưởng trên các hệ thống thông tin | *Hà Nội, ngày 24 tháng 04 năm 2024* |

Kính gửi:

- Đơn vị chuyên trách về CNTT/ATTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet và nền tảng số;
- Các Tổ chức tài chính, Ngân hàng thương mại;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

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 Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến 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: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Thứ trưởng Phạm Đức Long (để b/c);
- Cục A05 (Bộ Công an);
- Bộ Tư lệnh 86 (Bộ Quốc phòng);
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Toàn án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Trung tâm VNNIC, Trung tâm Thông tin;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG**
**PHÓ CỤC TRƯỞNG**

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

**Trần Đăng Khoa**

**Phụ lục**
**THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC**
*(Kèm theo Công văn số /CATTT-NCSC ngày / /2024 của Cục An toàn thông tin)*

**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 | 5e37b3289054d5e774c02a6ec491 5a60156d715f3a02aaceb7256cc3e bdc6610 |
| Cheat.Lab.2.7.2.zip | https[:]//github[.]com/microsoft/vcpkg/files/1412 5503/Cheat.Lab.2.7.2.zip |
| lua51.dll | 873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749 d7631f2912bcb640439997 |
| readme.txt | 751f97824cd211ae710655e60a26885cd79974f0f 0a5e4e582e3b635492b4cad |
| compiler.exe | dfbf23697cfd9d35f263af7a455351480920a95bfc 642f3254ee8452ce20655a |

| | |
|---|---|
| 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/