

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	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[.]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-anovel-approach/>