**RAT:**

Tạo socket trên máy bị nhiễm cho phép các máy tấn công kết nối vào (sử dụng winsock), do ở trên máy bị nhiễm nên có quyền tạo process cmd cho phép attacker thực thi câu lệnh bất kì.

Máy client (attacker) có thể kết nối thông qua lệnh telnet:

Ví dụ: telnet DESKTOP-VES4POV 1999

1999 là cổng được mở từ rat.

**Credential Dump:**

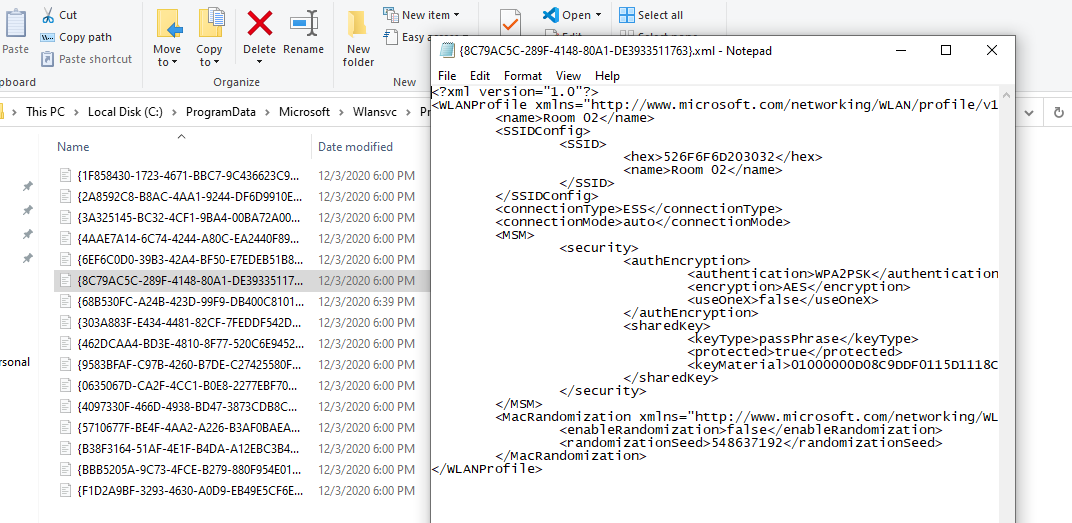
Là kĩ thuật ăn cắp các thông tin nhạy cảm ở trong máy.

Kỹ thuật này cho phép hacker lấy được thông tin đăng nhập của nhiều tài khoản từ một người. Và những thông tin này có thể là bất cứ thứ gì như ngân hàng, tài khoản email, tài khoản facebook, wifi, github,…

Ví dụ như mật khẩu wifi được lưu ở trong 1 file xml ở trong path:

**C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\...**

**Trích xuất các thông tin từ trong file xml này ra gọi là credential dump.**



Sử dụng thư viện #include <wincred.h> để code.