TROJAN THƯ RÁC TINH VI CHƯA TỪNG CÓ

Chuyên

Chuyên gia bảo mật kỳ cựu Joe Stewart tưởng rằng mình đã thông tường mọi nhẽ về malware, cho tới khi ông bắt gặp SpamThru Trojan- một chương trình phá hoại được thiết kế để phát tán thư rác từ máy tính bị nhiễm.

Sử dụng công nghệ P2P để gửi lệnh tới cho các PC bị hijack, Trojan này được trang bị hẳn một ... máy quét virus riêng, với mức độ phức tạp và tinh vi ngang ngửa với các phần mềm quét virus chính thông.

"Đây là lần đầu tiên tôi bắt gặp hiện tượng này", Stewart thốt lên. Ông hiện đang làm chuyên gia bảo mật cao cấp của SecureWorks.

"Mục đích của máy quét virus này, đơn giản là để tự bảo vệ mọi "nguồn lực" của Trojan. Trong trường hợp nó phải cạnh tranh với một virus gửi mail hàng loạt chẳng hạn, nó sẽ loại bỏ được đối thủ đáng ghét".

Nguồn: codycafe

Đại đa số các virus và Trojan hiện nay chỉ tìm cách chặn các phần mềm diệt virus tải các phiên bản update nhưng chiến đấu với cả các malware đối thủ kiểu này thì đúng là "hiếm có khó tìm", nếu chưa muốn nói là trường hợp đầu tiên. SpamThru đã nâng cuộc chơi lên một tầm mới - sử dụng nguyên một công cụ diệt virus để tiêu diệt "đồng đảng".

Tuy nhiên, động cơ của nó thì chẳng khó hiểu chút nào. Máy tính thì chỉ có một mà hacker nào cũng muốn giành lấy quyền kiểm soát. Lẽ tất yếu, các hacker sẽ đấu đá với nhau, tìm mọi cách tiêu diệt các malware khác bằng cách xóa bỏ registry key hoặc lừa cho malware khác nghĩ rằng ...

chúng đã đang chạy rồi.

Thông minh và táo tợn

Ban đầu, Trojan này sẽ tải một DLL từ máy chủ trung ương điều khiển của hacker. Sau đó, nó sẽ tải về máy tính bị nhiễm một bản lậu của Kaspersky Antivirus. 10 phút sau khi download DLL, nó bắt đầu scan hệ thống để lùng diệt các malware khác và bỏ qua những file "nhà mình".

"Bất cứ malware nào bị phát hiện cũng sẽ bị Windows xóa hết trong lần khởi động lại sau đó", Stewart giải thích. Ngay bản thân ông lúc đầu cũng bị bối rối với mục đích của hacker khi cài đặt phần mềm scan virus Kaspersky.

"Tôi chỉ nghĩ đơn giản là nó đang ngụy trang mộtc ách thông minh. Nhưng phải đến khi phân tích kỹ hơn, tôi mới nhận ra một cơ chế hoạt động vô cùng tinh vi mà hacker đã nghĩ ra để có thể chiếm trọn băng thông cho thư rác của hắn".

Chưa hết, SpamThru còn sử dụng một cơ cấu ra lệnh và kiểm soát cực kỳ khéo léo để tránh bị shutdown. Nó sử dụng một giao thức P2P tùy biến để chia sẻ thông tin với các peer khác, bao gồm địa chỉ IP, các cổng và phiên bản phần mềm của máy chủ điều khiển.

Trong trường hợp máy chủ điều khiển bị tắt, spammer sẽ có thể cập nhật toàn bộ các thông tin này lên một máy chủ điều khiển mới trong mạng peer.

Các thư rác mà SpamThru phát tán đi đều dựa trên template có sẵn nhưng với các cụm từ ngẫu nhiên trong nội dung, tên người gửi ngẫu nhiên. Những template này đều được mã hóa và sử dụng một phương pháp xác thực đặc biệt, ngăn không cho kẻ khác download ké.

Chưa hết, nó còn có thể thay đổi cả chiều rộng và chiều cao của hình ảnh GIF nhằm qua mặt các bộ lọc.

Trọng Cầm