MÃ PHÁ HOẠI BẢO MẬT NGUỴ TRANG MỚI CỦA HACKER

Bí mật không phải là trò chơi gây ngạc nhiên xây dựng nên để né tránh phần mềm diệt virus

Hiện nay các hacker đang xây dựng phần mềm mới giúp ẩn giấu mã tấn công trình duyệt trước một số kiểu phần mềm bảo mật.

Phần mềm này có tên gọi VoMM (eVade o' Matic Module), sử dụng nhiều kỹ thuật tổng hợp khác nhau từ các mã khai thác đã biết khiến một số kiểu phần mềm diệt virus không thể nhận ra.

Sử dụng các kỹ thuật này, VoMM "có thể tạo ra số lượng vô hạn biến thể của một lỗ hổng khai thác", Aviv Raff - một trong những người phát triển đằng sau dự án này nói.

"Mục đích của nó là cung cấp một số kỹ thuật ngoại lệ khiến hầu hết các mã khai thác trình duyệt không thể bị dò tìm", một hacker khác có bí danh "LMH" viết trên blog của một trong những người thành lập dự án.

Người dùng phần mềm sẽ gặp phải công nghệ scripting server-side, tự tạo ra phiên bản mới cho mã khai thác và phát tán chúng vào người dùng trình duyệt khi họ ghé thăm website của hacker. Bằng cách tạo ra một số thay đổi "mang tính thẩm mỹ" trên mã nguồn khiến nó không tự tác động lên chính chức năng của mình, VoMM tạo ra các bản sao phần mềm độc hại không thể bị dò tìm bằng kỹ thuật "signature - based" (dấu hiệu cơ bản).

Các phần mềm diệt virus theo kiểu "signature - based" có thể phân tích được các malware đã biết. Sau đó tạo ra một "dấu vân tay số" cho phép phần mềm diệt virus xác định mã độc hại. Bằng cách thêm vào các thành phần mở rộng (tab, space, comment ngẫu nhiên và các tên khác nhau) không nằm trong những dấu hiệu đã biết, VoMM tạo ra phần mềm có thể né tránh sự dò tìm.

VoMM có thể sẽ được xây dựng modul mới trong phiên bản v3.0 sắp tới, sử dụng bộ công cụ hacking Metasploit vốn đang được dùng hết sức rộng rãi hiện nay. Được biết hãng phát triển Metasploit, HD Moore cũng đang phát triển VoMM.

T.Thu