PHẦN MỀM ĐỘC HẠI CŨNG... MÃ NGUỒN MỞ

Những kẻ chuyên lập trình các phần mềm độc hại cũng đang dần chuyển sang ứng dụng các giải pháp mã nguồn mở vào trong công việc của chúng. Hiểm hoạ gia tăng Trong "Bản báo cáo hiểm hoạ bảo mật toàn cầu 2006", hãng bảo mật McAfee cảnh báo ng&agr

Những kẻ chuyên lập trình các phần mềm độc hại cũng đang dần chuyển sang ứng dụng các giải pháp mã nguồn mở vào trong công việc của chúng. Hiểm hoạ gia tăng Trong "Bản báo cáo hiểm hoạ bảo mật toàn cầu 2006", hãng bảo mật McAfee cảnh báo ngày càng có nhiều tin tặc chia sẻ mã nguồn và ý tưởng một cách rất tự do. Trong đó có cả việc chia sẻ những mã nguồn, tài liệu kỹ thuật và cả những chú thích về cách thức vận hành của các đoạn mã. Với những tài liệu này, các tác giả hoàn toàn có thể dễ dàng chính sửa phát triển theo cách riêng của họ. Hiểm hoạ đe doạ bảo mật toàn cầu cũng vì thế mà ngày càng tăng. McAfee nhấn mạnh đây là một cách thực sự rất hiệu quả trong việc phát triển các loại mã nguồn - kể cả mã nguồn phần mềm hợp pháp lẫn phần mềm độc hại. "Cũng giống như bất kỳ một công cụ hỗ trợ mạnh mẽ nào khác, mã nguồn mở cũng có thể được sử dụng cho những mục đích ác ý khác - cụ thể là trong lĩnh vực bảo mật," McAfee cảnh báo. Ứng dụng các giải pháp mã nguồn mở hoặc chia sẻ mã nguồn là một điều vô cùng thuận lợi cho sự phát triển của những đối tượng "script kiddies" hay là những kẻ chỉ có hiểu biết hạn chế trong lĩnh vực lập trình, gồm cả lập trình phần mềm độc hại. Giờ đây chúng sẽ thấy dễ dàng trong việc tải về các tài liệu và đoạn mã để phát triển thêm thành các phiên bản phần mềm độc hại khác. Cộng đồng virus ... mở Ngoài ra, báo cáo của McAfee còn cho rằng xu hướng thành lập các cộng đồng ảo hoặc chia sẻ thông tin qua các kênh IRC (Internet Relay Chat) cũng đang nổi lên mạnh mẽ trong giới lập trình virus - nhất là những kẻ có liên quan đến các nhóm tội phạm mạng có tổ chức. Tuy nhiên, những nhóm đối tượng như vậy sẽ rất khó gia nhập được các cộng đồng mã nguồn mở do tâm lý của chúng là cần phải tránh thu hút sự chú ý của các cơ quan bảo vệ luật pháp. Phát triển phần mềm độc hại cũng là một vòng phát triển lâu dài - ở đó các đoạn mã được phát triển, các lỗi được sửa, rồi cũng có bản thử nghiệm (beta) và bản chính thức được phát hành trong cộng đồng phát triển phần mềm độc hại. Quá trình này hoàn toàn giống với quá trình phát triển phần mềm trong những cộng đồng mã nguồn mở hợp pháp. "Chúng ta hoàn toàn có thể nói giải pháp mã nguồn mở đã cho phép chúng tạo nên những cuộc tấn công có chất lượng và hiệu quả cao hơn," McAfee cảnh báo. "Xu hướng của ngày nay là phát triển nhóm". Các công cụ hacker cũng được sáng tạo ra và phân phát miễn phí theo mô hình mã nguồn mở, McAfee cho biết. Lấy ví dụ các phiên bản của SDBot - một con trojan có khả năng mở một cổng hậu (backdoor) trên các hệ thống bị nhiễm - thực sự là một phần bổ sung của bộ công cụ hacker FU. Công cụ này có thể tìm thấy ở bất cứ đâu trên Internet. Không những thế, McAfee cho biết, nếu dành thời gian chúng ta có thể tìm thấy rất nhiều các loại công cụ độc hại khác trên Internet. Trong khi đó, hiện có rất ít tác giả lập trình virus "cống hiến" thời gian để sáng tạo và sửa lỗi một con virus hoàn toàn mới từ con số 0. Tin tặc giờ cũng hoạt động như các nhà tư vấn, cung cấp đầy các hướng dẫn khi chúng quyết định mở cửa mã nguồn phần mềm độc hại. "Đây là một giải pháp rất hiệu quả cho việc phát triển các phần mềm độc hại," McAfee kết luận. Hoàng Dũng