# CỨ 6 PC CÓ 1 BỊ NHIỄM ROOTKIT

Những

Những chuyên gia phân tích bảo mật của hãng Prevx đã cảnh báo người dùng máy tính, đặc biệt là các hệ thống của doanh nghiệp đang bị đe dọa bởi sự phát triển "cực độ" của những phần mềm rootkit.

Hơn 725.000 máy tính được quét bằng công cụ dò tìm phần mềm độc hại Prevx CSI Malware scanner trong một giai đoạn là 2 tháng đã nhận dạng được nhiều hình thức malware và spyware khác nhau, theo tỉ lệ cứ 6 PC thì có 1 đã lây nhiễm. Đặc biệt là những máy tính trong hệ thống của các doanh nghiệp có tỉ lệ bị nhiễm rootkit cao hơn cả.

Theo thống kê của Prevx, con số máy tính lây nhiễm rootkit đã tăng từ 15.6% trong tháng 10 lên 22% vào đầu tháng 12. "Bóng tối rootkit đang bắt đầu bao phủ lên kỷ nguyên máy tính", chuyên gia Jacques Erasmus của Prevx dí dỏm nhận định. "Phải thật cảnh giác và có giải pháp bảo mật thích hợp để phòng chống rootkit hiệu quả".

Rootkit là các chương trình rất "ma mãnh". Sau khi xâm nhập vào máy tính, chúng tự điều chỉnh để giấu mình trước người dùng và cả những chương trình bảo mật khác đã cài đặt sẵn trên hệ thống. Nằm ẩn mình trên hệ thống, rootkit âm thầm ghi lại, hiệu chỉnh, đánh cắp thông tin dữ liệu từ máy tính nạn nhân. Không phải chương trình anti-virus nào cũng có thể dò tìm được rootkit trên hệ thống nên đôi khi người dùng vẫn tin rằng máy tính của mình "sạch" và thiếu cảnh giác với những thông tin tài chính, dữ liệu cá nhân có giá trị.

Mã độc có thể được phát tán qua bộ nhớ đệm công cụ tìm kiếm

Rootkit, "kẻ trộm" cao tay cần cảnh giác ngăn chặn.

Theo hãng bảo mật Aladdin, bộ nhớ đệm (cache) của những công cụ tìm kiếm (search engine) hàng đầu là Google, Yahoo và MSN Live vẫn cung cấp một nơi ẩn chứa cho... mã độc. Hãng này thường xuyên ghi nhận lại một cuộc tấn công vào website trường đại học mà dấu vết xuất phát từ bộ nhớ đệm "nhiễm độc". Website này đã bị ngưng hoạt động nhưng mã độc từ nó vẫn được phát tán thông qua bộ nhớ đệm của công cụ tìm kiếm.

Hãng bảo mật Aladdin không chỉ cụ thể công cụ tìm kiếm nào đã phát tán mã độc từ website trên nhưng cho biết cả 3 công cụ tìm kiếm hàng đầu hiện nay là Google, Yahoo và MSN Live đều bị trường hợp trên. Những trang được lưu vào bộ nhớ đệm có thể "sống" từ vài tuần thậm chí vài tháng cho đến khi phần lưu trữ bộ nhớ đệm được làm mới trở lại (refresh).

Hầu hết các website chứa mã độc đều có một phiên bản sao chép trên máy chủ bộ nhớ đệm của các công cụ tìm kiếm. Tuy vậy, những nhà quản lý công cụ tìm kiếm vẫn chưa có động thái gì để xử lý vấn đề này. Hơn hết, người dùng Internet vẫn phải luôn cảnh giác các website lạ và không bao giờ tắt chương trình anti-virus hay tường lửa trên máy khi duyệt web.

Tuyết Phấn