TOP 10 MÃ ĐỘC NGUY HIỂM NHẤT THÁNG 2

Hãng bảo mật của Anh Sophos

Hãng bảo mật của Anh Sophos vừa công bố danh sách Top 10 mã độc nguy hiểm nhất tháng 2. Theo đó vị trí đầu tiên lại thuộc về một cái tên mới tinh.

Cái tên đó thuộc về một dòng mã độc hoàn toàn mới có khả năng "thay đổi diện mạo" liên tục nhằm đánh lừa và qua mặt các phần mềm diệt virus.

"Đó là một giải pháp nguỵ trang hoàn toàn mới," chuyên gia tư vấn công nghệ cao cấp của Sophos Graham Cluley khẳng định. "Mã độc này sử dụng một bộ mặt để tấn công người dùng. Nhưng diện mạo của nó sẽ ngay lập tức thay đổi nếu lây nhiễm thành công giúp chúng nguy trang và tránh bị phát hiện."

"Cho đến lúc này chúng tôi đã phát hiện được hàng ngàn biến thể mới của dòng phần mềm độc hại Dref và Dorf. Thực chất chúng chỉ là một loại mã độc nhưng mang nhiều diện mạo khác nhau".

Những kẻ chuyên lập trình mã độc đã sử dụng một loại mã có tên HckPk. Mã này có thể dễ dàng được tìm thấy trên mạng Internet. Chỉ cần bổ sung thêm đoạn mã này vào là "tác phẩm" của chúng đã có được tính năng thay đổi diện mạo nguy hiểm nói trên.

"Cộng đồng hacker gần như không ai không biết đến HckPk. Công việc còn phải làm của hacker chỉ là "đóng gói" lại sản phẩm của chúng. Mỗi khi cần thay đổi để qua mặt phần mềm diệt virus thì hacker chỉ cần thay đổi chút ý mã nguồn HckPk là đã có thể tạo ra một biến thể hoàn toàn mới," chuyên gia Cluely cho biết.

Con số thống kê của Sophos cho thấy mã độc HckPk chiếm tới hơn một nửa trong số các mã độc được phát hiện trong tháng 2. Như chỉ tính riêng dòng sâu Dref và Dorf đã có 6.000 biến thể khác nhau xuất hiện trong tháng 2. Tiếp theo là dòng sâu Storm Worm với hơn 1.500 biến thể. Những dòng sâu này đều được sử dụng mã độc HackPk.

"Phát hiện được mã độc này là một thành công đối với các hãng bảo mật. Đó là minh chứng cho thấy các hãng bảo mật đang ngày càng chủ động trong việc chống lại các mã độc mới. Nhưng bên cạnh đó giới lập trình virus cũng ngày một trưởng thành và trở nên chuyên nghiệp hơn".

Các chuyên gai phân tích cho biết HckPk xuất hiện trong khoảng cuối năm 2006. Tuy nhiên, tại thời điểm đó nó chưa "khẳng định được khả năng của mình". Gần đây nó bắt đầu nổi lên.

Những vị trí còn lại trong bảng xếp hạng vẫn thuộc về những tên tuổi quen thuộc như Netsky, Mytob, Nyxem ...

Tỉ lệ email nhiễm mã độc tháng qua vẫn được duy trì ở mức thấp, vào khoảng một trong 256 email là có chứa mã độc. Trong tháng 2, Sophos phát hiện được tổng cộng 7.757 mã độc mới.

STT

Mã độc

Tỉ lệ (%)

1

HckPk

50,3

2

Netsky

15,1

3

Mytob

12,5

4

Zafi

4,8

5

Sality

3,8

6

MyDoom

3,0

7

Bagle

2,4

8

Clagger

1,4

9

Nyxem

1,1

10

StraDl

1,0

Khác

4,6

Hoàng Dũng