HÃY CẨN THẬN VỚI TIN TẶC "BẮT CÓC TỐNG TIỀN"

Doanh nghiệp vừa và nhỏ nên back-up dữ liệu thật cẩn thận nếu không muốn trở thành nạn nhân của nạn "bắt cóc tống tiền" của bọn tin tặc. Đây là lời cảnh báo của hãng bảo mật Kaspersky Labs đã đưa ra cùng với việc cho công bố bảo báo cáo địn

Doanh nghiệp vừa và nhỏ nên back-up dữ liệu thật cẩn thận nếu không muốn trở thành nạn nhân của nạn "bắt cóc tống tiền" của bọn tin tặc. Đây là lời cảnh báo của hãng bảo mật Kaspersky Labs đã đưa ra cùng với việc cho công bố bảo báo cáo định kỳ hàng quí về phần mềm độc hại. Con số kỷ lục Trong bản báo cáo đó, Kaspersky Labs khẳng định số lượng các loại phần mềm độc hại "bắt cóc tống tiền" (ransomware) - hay là những phần mềm độc hại có khả năng thu thập, mã hoá thông tin và đòi nạn nhân phải trả một khoản tiền mới chịu trả lại dữ liệu. Không những thế, các thuật toán mã hoá cũng đang ngày càng trở nên phức tạp hơn. Thống kê của Kaspersky con số nạn nhân của phần mềm ransomware đã đạt đến con số kỷ lục trong quí II năm 2006. Loại phần mềm độc hại này lần đầu tiên xuất hiện là vào đầu năm 2005. Công nghệ mã hoá - Cuộc chơi mèo đuổi chuột Ban đầu, ransomware mới chỉ sử dụng các thuật toán mã hoá đơn giản để "bắt cóc" các tệp tin và đòi tiền chuộc. Tuy nhiên, trong những vụ tấn công gần đây, trong các phần mềm ransomware đã có sự xuất hiện của công nghệ mã hoá RSA và tin tặc cũng đã bắt đầu sử dụng các giải pháp bảo vệ mật khẩu và giấu tệp tin phức tạp hơn. Kaspersky cho rằng kẻ tấn công và các hãng bảo mật hiện trong rơi vào tình thế chơi trò "mèo đuổi chuột" - ở đó các hãng bảo mật nghiên cứu bẻ khoá phần mềm ransomware còn tin tặc kẻ tìm cách ứng dụng các giải pháp mã hoá phức tạp hơn. "Vẫn có những tình huống mà ở đó các hãng bảo mật không thể giải mã được những tệp tin đã bị bắt cóc," Davide Emm - chuyên gia tư vấn công nghệ cao cấp của Kaspersky - khẳng định. "Trong những công ty lớn, phòng ban phụ trách vấn đề công nghệ thông tin sẽ thường xuyên back-up lại dữ liệu. Chính vì thế mà mối đe doạ chủ yếu nhằm vào các doanh nghiệp nhỏ và người dùng cá nhân, do những đối tượng này thường không mấy chú trọng đến vấn đề back-up dữ liệu." Lấy ví dụ, biến thể mới nhất của Gpcode ransomware đã sử dụng khoá mã hoá 660-bit. Với khoá mã này các chuyên gia nghiên cứu cho rằng cần phải mất ít nhất 30 năm để bẻ khoá mã này với một chiếc máy tính chạy ở tốc độ 2.2GHz. Giới hạn của công nghệ Tuy nhiên, dựa trên những nghiên cứu, Kaspersky đã có thể bẻ được khoá mã đó và bổ sung các biện pháp bảo vệ cho phần mềm bảo mật của hãng. Trong khi Kaspersky đã có thể bẻ được những khoá mã trên thì các chuyên gia nghiên cứu lại tin tưởng rằng các giải pháp mã khoá đã đạt đến giới hạn của công nghệ mã hoá hiện đại ngày nay. Như vậy sẽ đồng nghĩa với việc nếu xảy ra các vụ tấn công trong tương lai, chúng ta sẽ có có thể bẻ mã khoá thành công được. Đồng nghĩa với việc nạn nhân của vụ bắt cóc tống tiền sẽ phải trả tiền để nhận lại dữ liệu của mình. Tác giả của các phần mềm ransomware Cryzip và Krotten - những phần mềm ransomware sử dụng kỹ thuật phổ biến nhất - hiện vẫn chưa bị bắt. Tuy nhiên, cho dù chúng có bị bắt thì thành quả công việc của chúng cũng vẫn sống mãi trong giới tin tặc. Những kẻ sẽ phát triển thêm dựa trên nền tảng của Cryzip và Krotten. Ransomware rõ ràng sẽ còn là một vấn đề đau đầu của ngành công nghiệp bảo mật trong một thời gian dài nữa. Hoàng Dũng