Logo Logo not found or type unknown

Phần mềm diệt virus không hiệu quả! Vì sao vẫn phải dùng?

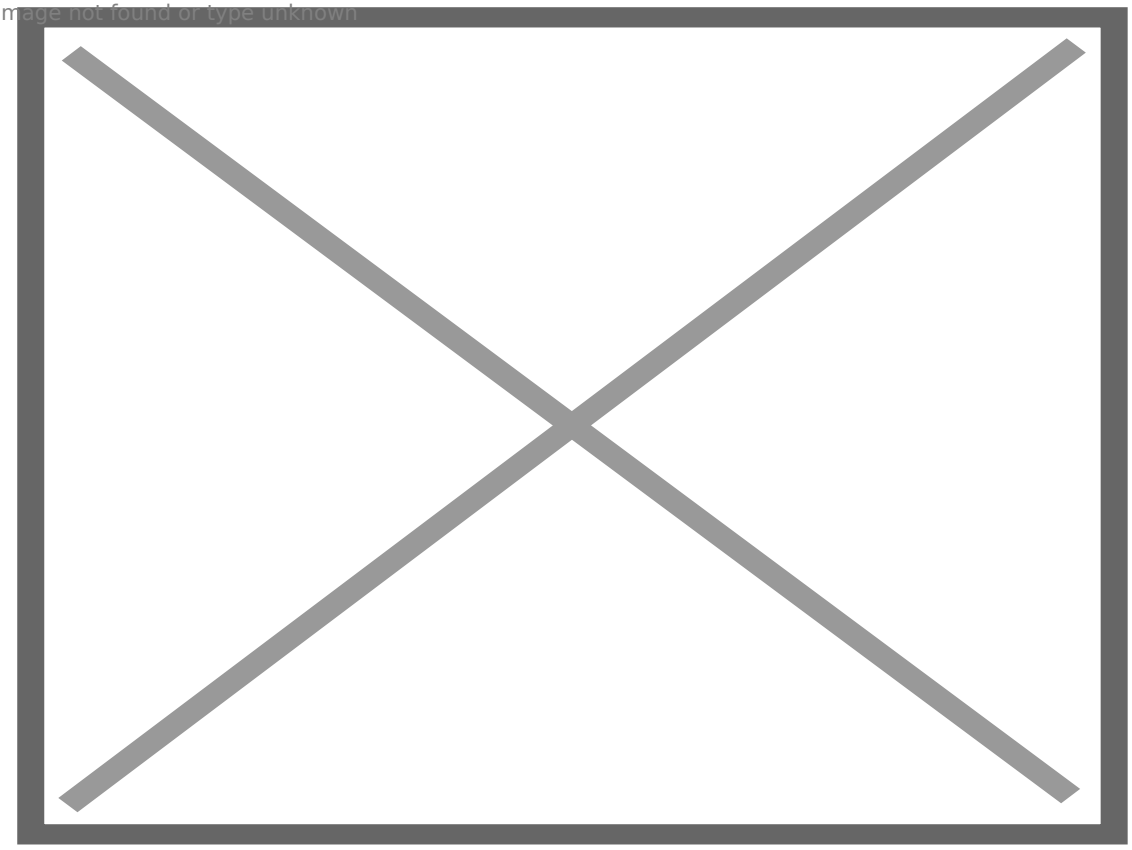
16:20 30/09/2016

Tác giả: Sv Thế Anh

Đánh giá đúng vai trò của phần mềm diệt virus trong một chiến lược tổng thể, doanh nghiệp mới có thể chuẩn bị sẵn sàng cho việc đối phó những mối đe doạ bảo mật của hôm nay và ngày mai

Trong nhiều năm, các công ty luôn tin cậy vào các phần mềm diệt virus để phát hiện, phòng tránh và gỡ bỏ mã độc trước khi chúng có thể gây rắc rối. Tuy nhiên, giờ đây, một phần mềm diệt virus không còn là giải pháp hiệu quả để giữ an toàn cho các hệ thống máy tính – đặc biệt là khi hàng loạt các loại keylogger, phần mềm gián điệp, sâu phá hại, Trojan... liên tục rình rập. "*Rõ ràng các giải pháp chống phần mềm gây hại dựa trên dấu hiệu nhận biết theo cách truyền thống đang ngày càng trở nên kém hiệu quả*" – theo ý kiến của một nhà phân tích từ Gartner. "*Trong những trường hợp doanh nghiệp đối mặt với cuộc tấn công mạnh mẽ, nó có thể không đem lại sự bảo vệ nào. Và trong những trường hợp khi người dùng cuối trở thành mục tiêu, việc chạy máy tính với quyền quản trị tối đa và bị lừa để kích hoạt một loại Trojan nào đó, các giải pháp chống mã độc truyền thống gần như không đem lại hiệu quả*". Câu hỏi đặt ra là, tại sao các doanh nghiệp vẫn sử dụng chúng?

Image not found or type unknown

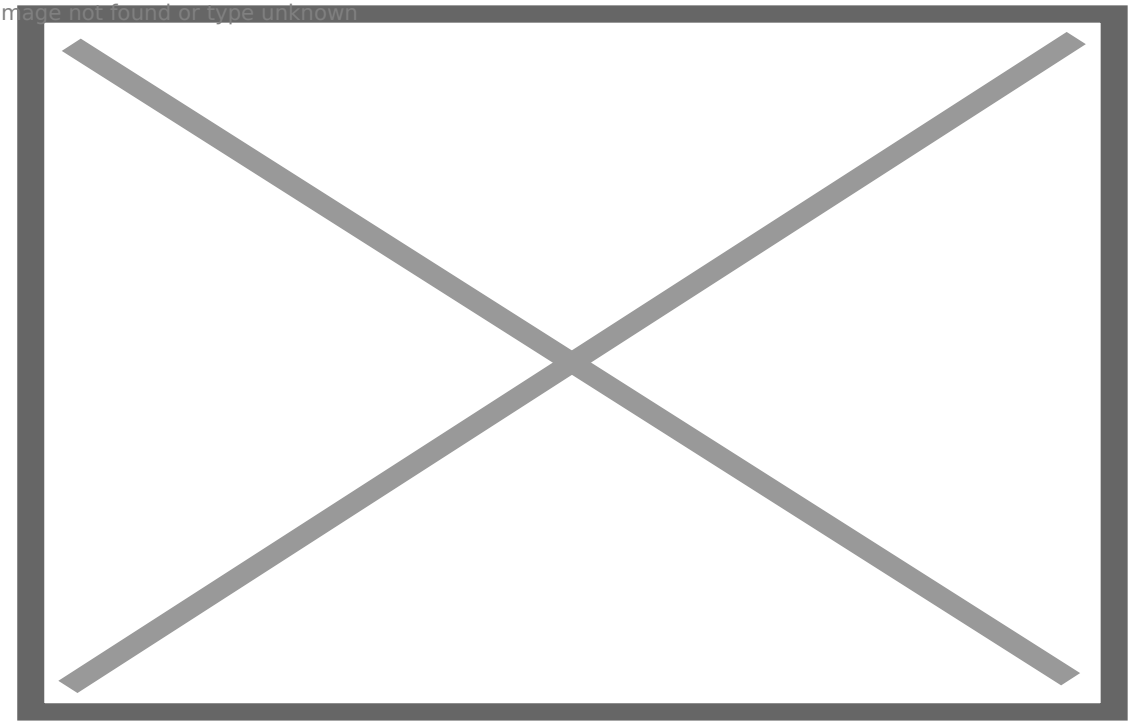


Phần mềm diệt virus trong bối cảnh hiện đại có gì khác biệt?

Tại sao các công ty vẫn tin cậy phần mềm diệt virus?

Thực tế, có nhiều lý do để các phần mềm diệt virus vẫn được triển khai trên hệ thống các công ty. Lý do trước hết chính là yêu cầu mang tính pháp lý và nhiều lý do nội bộ khác. Toàn bộ các công ty "*vẫn cần một thứ gì đó mang tên diệt virus trên danh mục sử dụng*" – nhà phân tích nhận định. "Các doanh nghiệp hoạt động theo pháp lý thực tế không có lựa chọn nào bởi luật yêu cầu điều đó. Các công ty khác dường như thiếu trách nhiệm và rất có thể phải đối mặt với những vụ kiện hoặc rủi ro với bảo hiểm nếu họ không sử dụng phần mềm diệt Virus trong công việc hàng ngày" – ông bổ sung thêm.

Image not found or type unknown



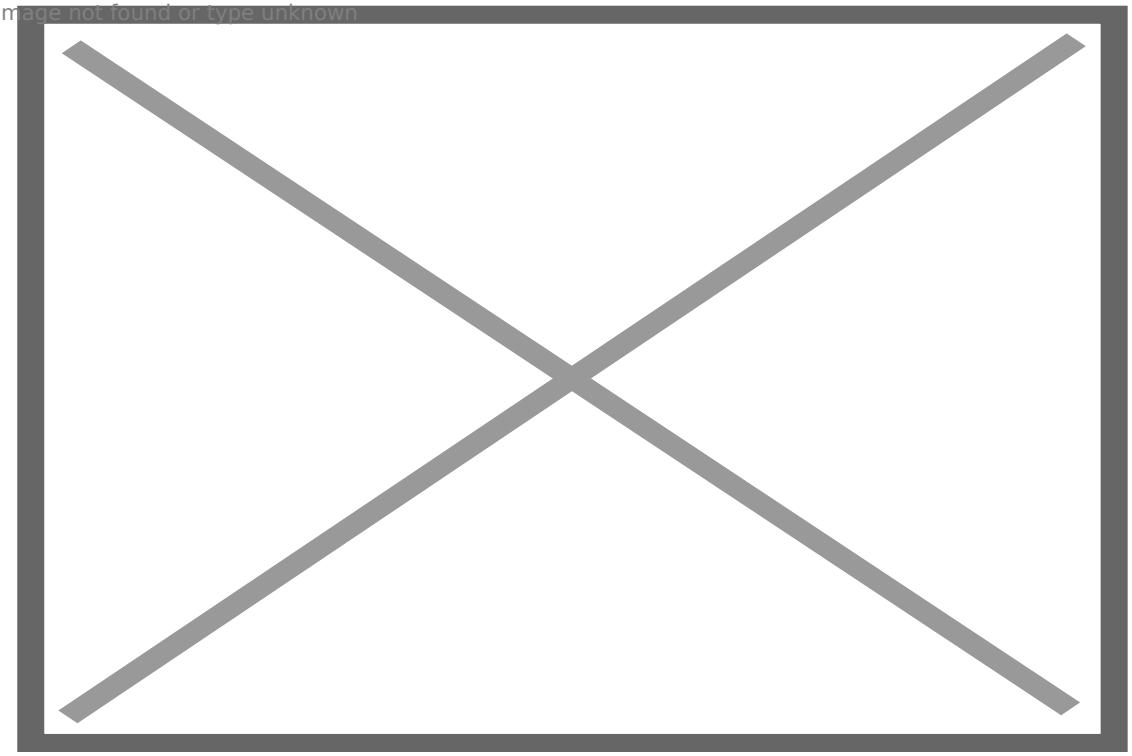
Các nhà cung cấp sản phẩm diệt virus cũng đang nỗ lực chuyển mình trước các mô hình tấn công hiện đại

Bản thân các phần mềm diệt virus vẫn được đưa vào sử dụng bởi lẽ "có quá nhiều các loại mã độc đang tồn tại" – nhà phân tích của IDC phát biểu. *"Microsoft đã thực hiện rất nhiều các nghiên cứu để chỉ ra rằng những máy tính không có phần mềm diệt virus nào đều bị lây nhiễm với tỉ lệ cao hơn rất nhiều so với các máy được trang bị - bất kể thuộc thương hiệu nào*". Nếu một người dùng máy tính không sử dụng phần mềm diệt virus và duyệt web trong khoảng 1 tuần, "tôi tin rằng phần mêm diệt virus sẽ có hiệu quả rất cao, chặn đứng nguy cơ lây nhiễm một loại phần mềm độc cơ bản nào đó" – nhà phân tích nhận định. Ông cũng chỉ ra rằng các loại "phần mềm diệt virus dựa trên dấu hiệu nhận diện tiêu chuẩn sẽ là một phần trong hệ thống các giải pháp bảo mật phức tạp và toàn diện hơn rất nhiều".

Mặt khác, một bối cảnh thể hiện được sự hữu dụng của phần mềm diệt virus là khi "bạn tin rằng rủi ro đến với hệ thống của mình là rất thấp bởi mục đích sử dụng của những thiết bị này, cách chúng kết nối với mạng và các giải pháp bảo mật tăng cường dành cho chúng" – theo IDC. Về phía mình, nhà phân tích Gartner cũng đồng ý rằng phần mềm diệt virus vẫn có vai trò nhất định. "Nếu bạn có những dấu hiệu có thể nhận biết một vụ tấn công và ngăn cản được điều đó, hãy sử dụng chúng. Điều rõ ràng là nó không phải lúc nào cũng là tính huống xảy ra. Bạn phải chấp nhận rằng có một vài phần trăm trường hợp các vụ tấn công sẽ vượt qua cơ chế bảo vệ dựa trên dấu hiệu theo cách truyền thống, vì thế cần phải có những giải pháp bảo vệ tăng cường. Trong đó đáng chú

ý là khả năng theo dõi các hành vi bất thường của hệ thống – dấu hiệu rất có thể là của một vụ tấn công".

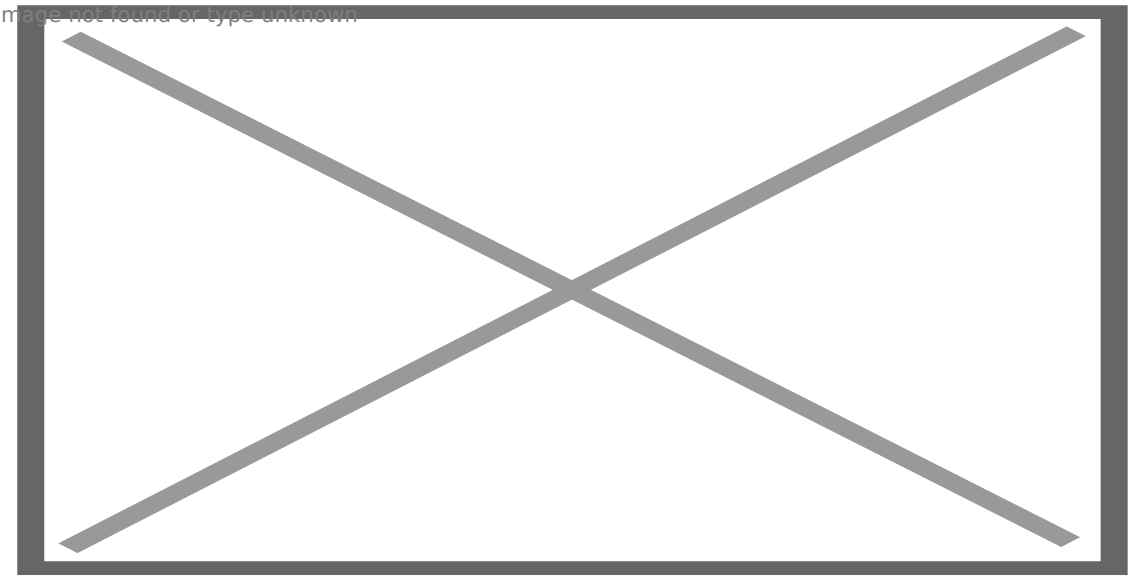
Image not found or type unknown



Các nhà phát triển phần mềm diệt virus đang làm gì?

Dĩ nhiên, điều đáng quan tâm bậc nhất chính là việc các nhà phát triển phần mềm diệt virus đang định hướng những "món" gì mới cho sản phẩm của mình nhằm khiến chúng trở nên hoàn hảo hơn. *"Tôi không suy nghĩ theo khái niệm chỉ giới hạn ở diệt virus nữa*" – nhà phân tích cho biết. "Đúng là vẫn có những sản phẩm diệt virus đơn thuần, tuy nhiên đó không phải là thứ phần lớn người dùng đang tìm kiếm". Thực tế, các phần mềm diệt virus đang dần trở nên phức tạp hơn với cơ cấu diệt virus đơn thuần theo kiểu truyền thống, phát hiện xâm nhập, tường lửa, quản lý hoạt động ứng dụng, giám sát lỗi hổng bảo mật... Mặc dù rất nhiều những thay đổi trong thị trường diệt virus đều được đưa ra bởi các gương mặt mới, nhiều cái tên lâu năm như *Symantec, McAfee, Kasspersky, Bitdefender, Sophos, Trend Micro...* cũng không ngồi yên. Ngược lại, họ đang rất nỗ lực để tích hợp các công nghệ bảo mật cao cấp vào sản phẩm hiện tại của họ. Thách thức đối với nhóm này nằm ở việc tích hợp các món mới vào những mã nguồn họ đang có và biến chúng thành thứ có thể quản lý được, tích hợp vào giao diện sử dụng hiện tại. Theo nhà phân tích, "họ cần phải tách rời những suy nghĩ về việc diệt virus theo kiểu truyền thống. Trong một số trường hợp, không chỉ những hãng cung cấp non trẻ mới đưa ra những phương thức tiếp cận và kĩ thuật mới để nhận diện và chặn đứng các mã độc mà chính việc tiếp thị và thương hiệu của những hãng lâu năm chưa thể hiện điều đó".

Image not found or type unknown

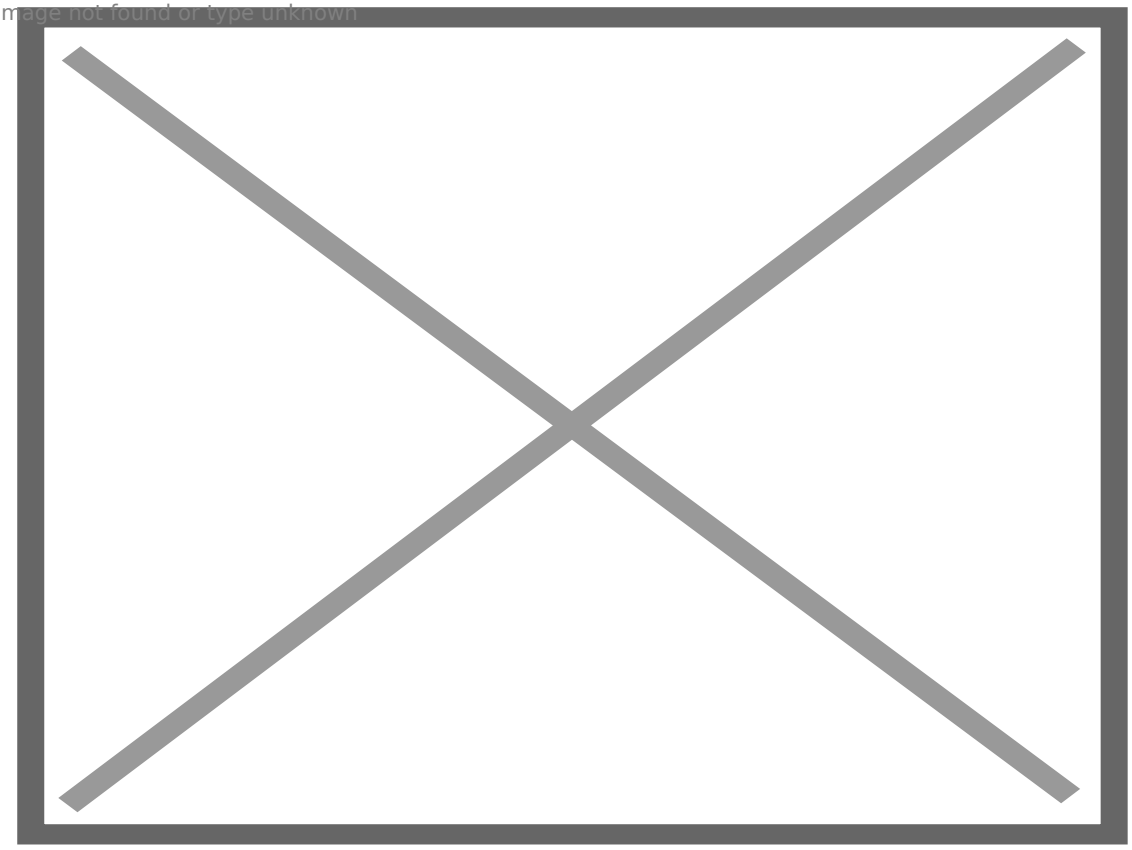


Khái niệm diệt virus trong bối cảnh mới cần được hiểu rộng hơn

Một số hướng tiếp cận khác

Theo phân tích, thị trường diệt virus hiện tại có thể được chia làm ba nhóm: truyền thống, bảo vệ hệ thống và giải quyết rắc rối. Trong đó, các sản phẩm truyền thống không thể phòng chống lại kẻ tấn công bởi chúng cũng có sản phẩm diệt virus trong tay và luôn đảm bảo các hàng rào này không thể phát hiện được công cụ tấn công trước khi tung ra sử dụng. Trong khi đó, các giải pháp bảo vệ hệ thống toàn diện lại hiệu quả hơn rất nhiều trong việc chặn đứng mã độc, các nhà phân tích cho rằng chúng không mạnh trong việc gỡ bỏ các yếu tố gây hại. Chính vì vậy, các giải pháp nhóm này chưa thể thay thế sản phẩm diệt virus truyền thống ở trên.

Image not found or type unknown



Cuộc chiến bảo mật chưa bao giờ nguội trong suốt lịch sử tồn tại của ngành công nghệ thông tin

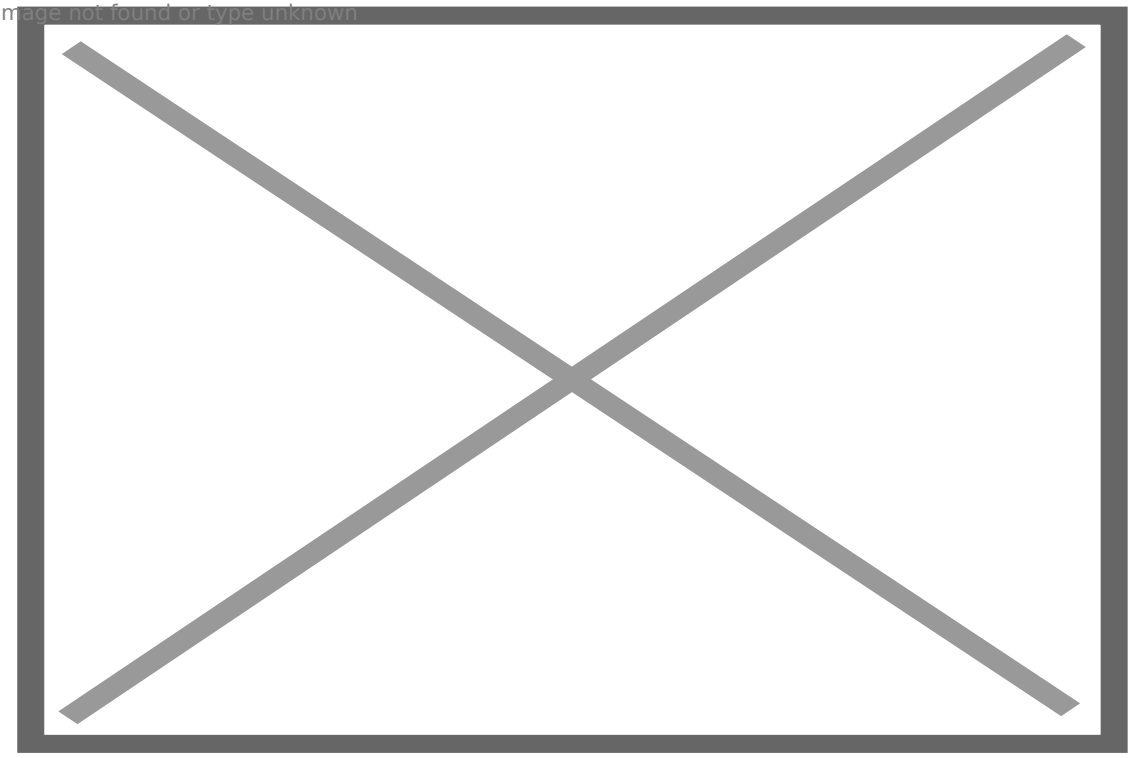
Tương tự như vậy, những sản phẩm tập trung vào việc giải quyết rắc rối cũng không quá hiệu quả trong việc cứu chữa những hệ thống bị lây nhiễm. Vì vậy, chúng cũng chỉ được coi là cơ cấu hỗ trợ cho các sản phẩm diệt virus. “Hiện tại, chúng ta chưa biết thị trường chống mã độc sẽ đi theo hướng nào, tuy nhiên tôi cho rằng đó sẽ là sự kết hợp của sản phẩm diệt virus để tạo ra thứ gì đó hiệu quả hơn – dù là thông qua những nghiên cứu nội bộ hoặc thâu tóm lẫn nhau” – một nhà phân tìch nhận định. “Chúng ta chắc chắn sẽ chứng kiến dấu chấm hết của khái niệm diệt virus mà chúng ta từng biết. Tuy nhiên trong thời đại mới, chúng ta sẽ vẫn thấy những kĩ thuật và các dấu hiệu cũ được sử dụng bởi nhiều nhà phát triển để hoàn thiện các kĩ thuật mới” – ông cho biết.

Cũng theo các chuyên gia, nhiều phát kiến mới trong thị trường bảo mật hiện nay được dẫn dắt bởi những gương mặt đơn lẻ như Webroot, Bit9/Carbon Black, Bromium, Triumfant, Invincea, Countertack, Cylance and Crowdstrike. “Một trong những nhà phát triển thành công hơn vào lúc này chính là hệ quả của sự kết hợp giữa Bit9 và Carbon Black. Trong đó, Bit9 cung cấp các giải pháp kiểm soát ứng dụng theo kiểu truyền thống còn Carbon Black có những thành phần nhận diện và phản ứng hệ thống (EDR)” – MacDonald phát biểu. “Kết hợp với nhau, họ cung cấp cơ chế bao gồm cả phát hiện và phòng chống cùng lúc”.

Mặt khác, những bước tiến công nghệ ở lĩnh vực này cũng nằm ở cơ chế hạn chế hoạt động ứng

dụng (sandboxing), giám sát bộ nhớ, cơ chế khoá khép kín, cơ chế tự học hỏi… Khía cạnh thú vị của sự đa dạng về các công nghệ tiềm năng này là nó khiến cho những kẻ xấu gặp khó khăn hơn nhiều trong việc tạo ra các loại mã độc đủ khả năng ẩn mình. Một số nhà phát triển mới cũng đang nỗ lực đưa các công nghệ chống mã độc mới tới với người dùng cuối chứ không chỉ các doanh nghiệp. Điều này cũng giúp giải quyết vấn đề bảo mật đối với các thiết bị cá nhân của họ trong môi trường làm việc (BOYD).

Image not found or type unknown



Sự phát triển của ngành công nghệ cũng đặt ra những nhiệm vụ mới với các chuyên gia bảo mật doanh nghiệp – điển hình là nhu cầu BYOD.

Vậy “con mồi” nên làm gì?

Như vậy, bất kể các nhà phát triển phần mềm diệt virus đang làm gì cũng như xu hướng phát triển thị trường công nghệ sẽ đi theo hướng nào, các nhà quản lý rủi ro, chuyên gia bảo mật cần phải tự tìm kiếm những hướng tiếp cận chủ động và nhiều tầng để gia cố hệ thống phòng thủ cho tổ chức của mình – những “con mồi” trước sự phát triển của các mối đe doạ hiện đại. Họ cần phải làm điều này thông qua việc tận dụng các công nghệ có thể khắc phục được quy mô tấn công đang ngày càng mở rộng hơn trên các hệ thống của doanh nghiệp. Theo thống kê,các nhà phân tích gợi ý rằng các công ty nên xem xét sử dụng công cụ bảo mật nhiều lớp để thu hẹp quy mô tấn công và đáp ứng được những yêu cầu khác biệt của máy chủ và máy đơn lẻ. Thực tế, cũng không ít các doanh nghiệp, tổ chức đang tìm cách thay thế những công cụ diệt virus của nhà cung ứng thứ ba

bằng các giải pháp bảo mật tích hợp trong hệ điều hành như danh sách “trắng” (cho phép) của ứng dụng, quản lý đặc quyền ứng dụng, bảo vệ tính toàn vẹn của ứng dụng, cách lý quyền thực thi của hệ thống...

Nhìn chung, chỉ có đánh giá đúng mức vai trò của phần mềm diệt virus trong một chiến lược tổng thể thay vì loại bỏ hoàn toàn chúng, các doanh nghiệp mới có thể chuẩn bị sẵn sàng cho việc đối phó những mối đe doạ bảo mật của hôm nay và ngày mai.

Nguồn: PCWorld

Link bài viết: https://nguoilambao.vn/phan-mem-diet-virus-khong-hieu-qua-vi-sao-van-phai-dung