2 LOẠI VIRUS CHUYÊN PHÁ HUỶ DỮ LIỆU

2 họ sâu máy tính sau đây thuộc dạng hoạt động theo chu kỳ, phát tán vào một ngày cố định hàng tháng. Chúng cực kỳ nguy hiểm bởi vì khi dữ liệu bị phá huỷ bởi 2 loại virus này thì không có khả năng phục hồi được. Họ sâu m&aacute

2 họ sâu máy tính sau đây thuộc dạng hoạt động theo chu kỳ, phát tán vào một ngày cố định hàng tháng. Chúng cực kỳ nguy hiểm bởi vì khi dữ liệu bị phá huỷ bởi 2 loại virus này thì không có khả năng phục hồi được. Họ sâu máy tính W32.Chir W32.Chir.B@mm là một loại sâu sâu máy tính lây lan qua e-mail. Nó thường sử dụng công cụ SMTP để gửi e-mai tới các địa chỉ email nó tìm được từ các loại files .wab, .adc, .db, .doc và .xls. Các email đính kèm các file nhiễm virus thường chứa nội dung như sau: From: @yahoo.com or imissyou@btamail.net.cn Subject: is coming! Attachments: PP.exe Khi máy bị nhiễm W32.Chir.B@mm nó tìm tất cả các ổ dữ liệu trong máy và tấn công vào các file có phần đuôi là tml, .exe, and .scr. Một đặc điểm cực kì nguy hiểm của nó là vào mùng 1 hàng tháng nó sẽ tự động ghi đè 4460 bytes các files có đuôi mở rộng là adc, .doc, and .xls làm cho không thể đọc được gì trong các file Word hoặc Excel đó và toàn bộ dữ liệu văn phòng của nạn nhân sẽ hoàn toàn không mở được. Mô tả chi tiết: Khi sâu máy tính hoạt động thì nó copy chính nó thành một tệp có tên là Runouce.exe vào thư mục C:\windows\system32 (với WinXP) hay C:\winnt\sytem32 (với Win2k) Đồng thời, sâu W32.Chir còn tạo thêm 1 khóa trong Registry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Runonce = Windows\System\Runouce.exe Do đó, phiên bản hoạt động của sâu máy tính luôn khởi động cùng với Windows . Cách Diệt Tải bản cập nhật offline hoặc phần mềm diệt virút của Symatec tại đây.- Tắt chế độ system restore - Khởi động lại chạy trong chế độ safe mode quét tất cả các ổ đĩa - Sửa lại registry bằng cách vào Start -> Run gõ regedit sau đó tìm key sau xóa đi: "Runonce = Windows\System\Runouce.exe" theo đường dẫn trong Registry là: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - Khởi động lại máy tính để hoàn tất quá trình. Họ sâu máy tính Worm/Generic (Theo cách đặt tên của AVG) Worm/Generic.FX!CME-24 là loại sâu máy tính lây lan qua đường email bằng các tệp đính kèm và phát tán cả trên mạng chia sẻ ngang hàng (P2P network). Vào ngày mùng 3 hàng tháng nó sẽ ghi đè lên các tệp có phần mở rộng là doc, xls, mdb, mde, ppt, pps, zip, rar, pdf, psd và dmp. Khi sâu máy tính hoạt động nó copy chính nó thành các tệp có tên là: Scanregw.exe, Net.exe, At.exe, Rundll16.exe vào thư mục hệ thống của Windows theo đường dẫn: C:\windows\system32 (với WinXP) và C:\winnt\sytem32 (với Win2k) Và đăng ký tệp scanregw.exe như một ScanRegistry trong khoá regedit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Thực hiện việc lây nhiễm của nó thông qua các địa chỉ email sưu tầm được, các tệp chứa thông tin email có đuôi như: HTM, DBX, EML, MSG, OFT, NWS, VCF, MBX, IMH, TXT và MSF. Nội dung thư có khuôn dạng địa chỉ người gửi là giả mạo (có thể là một địa chỉ không có thật). Tiêu đề và nội dung email được tạo ra ngẫu nhiên do con virut. File đính kèm có tên thay đổi nhưng phần mở rộng thường là *.pif hoặc *.scr, đôi khi phần mở rộng này còn bị ẩn đi. Cách diệt Tải bản cập nhật offline hoặc phần mềm diệt virút của Symatec tại đây.- Tắt chế độ system restore - Khởi động lại chạy trong chế độ safe mode quét tất cả các ổ đĩa - Sửa lại registry bằng cách vào Start -> Run gõ regedit sau đó tìm key có từ khóa sau xóa đi: Scanregw.exe, Net.exe, At.exe, Rundll16.exe theo đường dẫn trong Registry là: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - Khởi động lại máy tính để hoàn tất. Mẹo: Bạn cũng có thể đổi ngay ngày hệ thống về ngày mùng

4 tháng sau khi đang ở ngày cuối cùng của tháng hiện tại thì cũng có thể tránh được sự kích hoạt hoạt động của 2 loại sâu máy tính nói trên.