HAI SÂU MÁY TÍNH NGUY HIỂM LAN TRÀN TẠI VIỆT NAM

Theo cảnh báo của các chuyên gia bảo mật Công ty Misoft, Trendmicro hiện nay, các hệ thống mạng tại Việt Nam đang nhiễm nhiều hai loại sâu WORM_RONTOKBRO.B và WORM_RBOT.AZM. Sau đây chúng tôi xin cung cấp các thông tin về hai loại virus này để c&aacu
Theo cảnh báo của các chuyên gia bảo mật Công ty Misoft, Trendmicro hiện nay, các hệ thống mạng tại Việt Nam đang nhiễm nhiều hai loại sâu WORM_RONTOKBRO.B và WORM_RBOT.AZM. Sau đây chúng tôi xin cung cấp các thông tin về hai loại virus này để các bạn phòng chống máy tính và hệ thống mạng của mình. Sâu WORM_RONTOKBRO.B được đánh giá có mức độ nguy hiểm cao. Tốc độ lây nhiễm cao, lây nhiễm vào hệ điều hành: Windows 95, 98, ME, NT, 2000, XP, Server 2003. Phương thức phat tán: gửi bản sao của nó trong file đính kèm của email. File có chứa sâu sử dụng Biểu tượng thư mục của Microsoft để đánh lừa người dùng mở nó và sâu tiến hành các tấn công. Khá tinh vi, sâu cũng mở cửa sổ Windows Explorer nhằm che dấu các tiến trình nó thực hiện lên máy tính của nạn nhân. Sâu thả rất nhiều các bản sao của nó lên các thư mục với nhiều tên khác nhau. Trên các máy lây nhiễm chạy hệ điều hành Windows 2000, XP, and Server 2003, sâu thả bản sao vào đường dẫn được mã hóa cứng phía dưới thư mục User Profile. Sau đó tạo một thư mục trong đường dẫn này. Hiện tượng máy tính bị nhiễm sâu WORM_RONTOKBRO.B Loại sâu này sẽ thực hiện khởi động lại máy tính của nạn nhân khi thấy trên thanh tiêu đề (title bar) của cửa sổ có các cụm từ ".EXE" and "REGISTRY". WORM_RONTOKBRO.B chèn thêm lệnh PAUSE vào file AUTOEXEC.BAT (trong ổ đĩa C:\) khiến cho các máy bị nhiễm chạy Windows 95, 98, và ME bị tạm dừng trong quá trình khởi động, buộc người dùng phải ấn một phím bất kỳ để khởi động Windows. Đồng thời, sâu cũng thay đổi giá trị trong Registry làm mất mục Folder Options trên menu của tất cả các cửa sổ Windows Explorer và Control Panel. Do đó người dùng không thể mở được hộp thoại Folder Options. Đặc biệt hơn, WORM_RONTOKBRO.B làm vô hiệu hóa Registry khiến cho người dùng không thể mở cửa sổ Registry để thay đổi các giá trị mà sâu đã cấy thêm vào. Giải pháp diệt thủ công Bước 1: Khởi động ở chế độ Safe Mode » Trên Windows 95 1. Khởi động lại máy tính. 2. Bấm F8 ở màn hình Starting Windows 95. 3. Chọn chế độ Safe Mode từ Windows 95 Startup Menu sau đó bấm Enter. » Trên Windows 98 và ME 1. Khởi động lại máy tính. 2. Bấm phím CTRL cho đến khi menu startup xuất hiện. 3. Chọn chế độ Safe Mode sau đó bấm Enter. » Trên Windows NT (chế độ VGA) 1. Bấm Start>Settings>Control Panel. 2. Bấm nháy chuột vào biểu tượng System. 3. Bấm vào thanh Startup/Shutdown. 4. Đặt trường Show List là 10 giây và bấm OK để lưu sự thay đổi này. 5. Tắt máy và khởi động lại máy tính. 6. Chọn chế độ VGA từ menu startup. » Trên Windows 2000 1. Khởi động lại máy tính. 2. Bấm phím F8 cho đến khi nhìn thấy thanh Starting Windows ở cuối màn hình. 3. Chọn chế độ Safe Mode từ Windows Advanced Options Menu sau đó bấm Enter. » Trên Windows XP 1. Khởi động lại máy tính. 2. Bấm phím F8 sau khi Power-On Self Test (POST) được thực hiện. Nếu Windows Advanced Options Menu không xuất hiện, cố gắng khởi động lại máy và bấm phím F8 nhiều lần sau màn hình POST. 3. Chọn chế độ Safe Mode từ Windows Advanced Options Menu sau đó bấm Enter. Bước 2: Xoá các dấu vết ảnh hưởng đến quá trình khởi động máy tính trong Registry. 1. Mở Registry Editor. Chọn Start>Run, gõ Regedit, bấm Enter. 2. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau: HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run 3. Bên phải cửa sổ, tìm và xoá lối vào. •Trênd Windows ME, 2000, XP & Server 2003: Bron-Spizaetus = "%Windows%\INF\norBtok.exe" •Trên Windows 98 & NT: Bron-Spizaetus = "\INF\norBtok.exe"

(Lưu ý: %Windows% la`đương dẫ n măc định đến thư mục Windows, thông thương laC:\Windows hoặc C:\WINNT.) 4. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau: HKEY_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Run 5. Bên phải cửa sổ, tìm và xoá lối vào: •Trênd Windows 2000, XP & Server 2003: Tok-Cirrhatus = "%UserProfile%\Application Data\smss.exe" •Trênd Windows ME: Tok-Cirrhatus = "%Windows%\Application Data\smss.exe" Bước 3: Xoá các dấu vết cửa sâu trong Registry 1. Vẫ n trong cưa sổ Registry, bên trái, kích đúp để chọn đường dẫn sau: HKEY_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Policies>Explorer 2. Bên phải cửa sổ, tìm và xoá lối vào: NoFolderOptions = "dword:00000001" 3. Bên trái cửa sổ, kích đúp để chọn đương dẫn sau: HKEY_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Policies>System 4. Bên phải cửa sổ, tìm và xoá lối vào: DisableRegistryTools = "dword:00000001" 5. Đong cửa sổ Registry. Bước 4: Khôi phục lại file AUTOEXEC.BAT 1. Mơ file AUTOEXEC.BAT băng Notepad. Click Start>Run, gõ : notepad c:\autoexec.bat 2. Ấn Enter. 3. Xoá giá trị sau: pause 4. Đong file AUTOEXEC.BAT. 5. Click Yes để ghi lại. Lưu ý: Đối với các máy chạy Windows XP/ME ngắt tính năng System Restore. Về sâu WORM_RBOT.AZM Sâu WORM_RBOT.AZM có tốc độ lây nhiễm cao. Lây nhiễ m vaò HĐH: Windows 95, 98, ME, NT, 2000, XP, Server 2003. Sâu lây nhiễ m trên mạng chia sẻ. WORM_RONTOKBRO.B tha bản sao va`các thư mục được chia sẻ mặc định: •ADMIN$\system32 •C$\Windows\system32 •C$\WINNT\system32 Nếu thư mục đo có đặt password truy câp, sâu tập hợp trong danh sách ma`no định nghĩ a trước user ames va`passwords để thư truy câp lại. Nguy hiểm hơn, WORM_RONTOKBRO.B coì khai thăc các lỗ hổng để thực hiện phat tán các bản sao cửa no trong mạng: •LSASS Vulnerability •RPC/DCOM Vulnerability Ngoaì ra, loại sâu nay coì co khả năng ăn cắp ID cửa Windows trên may tính cửa nạn nhân va` CD key cửa nhiêù tro`chơi phổ biếnnhư FIFA, Command and Conquer, James Bond 007, Half-Life ....nếu như chúng được caî trên may bị nhiễ m. Giải pháp diệt thủ công Bước 1: Xác định va`dưng tiến trình hoạt động cửa Sâu: Dừng tiến trình hoạt động của sâu 1. Mở Windows Task Manager. »Trên Windows 95, 98, and ME, bấm CTRL+ALT+DELETE » Trên Windows NT, 2000, 2003 and XP, bấm CTRL+SHIFT+ESC, sau đó bấm vào mục Processes. 2. Trên danh sách các chương trình đang chạy, bấm nút End Task hay End Process, tuỳ thuộc vào phiên bản Windows đang chạy vơi tiến trình scrtkfg.exe. 3. Để kiểm tra liệu các chương trình virus đã dừng hay chưa, đóng Task Manager, sau đó mở lại lần nữa. 4. Đóng Task Manager. Bước 2: Xoá các dấu vết ảnh hương đến qua trình khơi đông may tính trong Registry. 1. Mở Registry Editor. Chọn Start>Run, gõ Regedit, bấm Enter. 2. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau: HKEY_CURRENT_USER>Software>Microsoft>OLE 3. Bên phải cửa sổ, tìm và xoá lối vào System CSRSS Patch = "scrtkfg.exe" 4. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau HKEY_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Run 5. Bên phải cửa sổ, tìm và xoá lối vào: System CSRSS Patch = "scrtkfg.exe" 6. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>RunServices 7. Bên phải cửa sổ, tìm và xoá lối vào: System CSRSS Patch = "scrtkfg.exe" 8. Đong cửa sổ Registry. Bước 3: Thiết lập lại cac giá trị bị sâu thay đổi trong Registry 1. Vẫ n trong cửa sổ Registry, bên trái, kích đúp để chọn đường dẫn sau: HKEY_LOCAL_MACHINE>Software>Microsoft>OLE 2. Bên phải cửa sổ, chuột phaì vaò EnableDCOM va`chọn Modify: 3. Bên trái cửa sổ, kích đúp để chọn đường dẫn sau: HKEY_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Run 4. Trong ô text box dươi Value Date, gõ Y: 5. Đong cửa sổ Registry. Lưu ý: Đối với các máy chạy

Windows XP/ME ngắt tính năng System Restore. Nếu chưa có phần mềm diệt virus nào của Trend Micro, bạn có thể vào http://housecall.trendmicro.com/ để tải về.
L.Quang