

BẢO VỆ MẠNG CỦA BẠN TRƯỚC SKYPE NHƯ THẾ NÀO

Ứng dụng

Ứng dụng tin nhắn tức thời (IP) và gọi điện thoại qua Internet (VoIP) Skype, từ chỗ chưa có người nào biết đến, nay đã có khoảng 150 triệu người dùng với 6 triệu người thường trực online chỉ trong vòng 3 năm. Và không tránh khỏi quy luật thông thường, Skype bị không ít đối tượng phá hoại nhòm ngó, tìm cách thâm nhập phá hoại. Một số vấn đề bảo mật xuất hiện, nhất là khi Skype được dùng trong các mạng doanh nghiệp lớn.

Trong nhận thức của nhiều người, Skype có thể là một lỗ hổng bảo mật, cho phép hacker lợi dụng để thâm nhập hệ thống. Họ cũng cho rằng nó mã hoá tất cả các liên lạc nên quá trình gửi tin không thể bị theo dõi, hay Skype sử dụng quá nhiều băng thông mạng và truyền tải các file nguy hiểm.

Skype không dễ quản lý. Nhưng nếu bạn lo lắng về Skype đang dùng trên mạng của mình, có nhiều phương pháp giúp bạn loại bỏ hoặc đảm bảo rằng nó an toàn. Chúng ta hãy cùng xem bạn có thể bảo vệ mạng của mình và người dùng Skype trước các nguy hiểm nó đem lại như thế nào.

Tìm người dùng Skype trên mạng

Việc đầu tiên cần phải làm là tìm ra ai đang sử dụng Skype trên mạng của bạn. Nếu bạn có một trong các chương trình ứng dụng quản lý cấu hình mạng như Microsoft SMS, LANDesk HP hay OpenView Client Configuration Manager, bạn đã có đủ công cụ trong tay. Hãy dùng chức năng dụng sẵn bên trong các ứng dụng đó.

Nếu không có ứng dụng nào như trên, đừng lo lắng. Bạn hãy tải một script mẫu có tên Skype_Check for Windows trên website SkypeTips.com và thực hiện các bước sau:

- Kiểm tra xem liệu Skype đã được cài đặt trên các máy trong mạng chưa và lập một báo cáo các hệ thống có nó.
- Ghi lại phiên bản của Skype.
- Kiểm tra xem liệu có proxy nào được thiết lập cho nó hay không.
- Kiểm tra cổng Skype đang dùng và ghi lại.
- Kiểm tra xem liệu cổng 80 có được phép sử dụng không và ghi lại.
- Kiểm tra cổng đang được dùng và cho phép bạn copy file XML Shared tổng hợp với các thiết lập chính xác.

- Kiểm tra và ngắt truyền tải file, ghi lại.
- Kiểm tra và ngắt Skype API, ghi lại.

Bạn có thể dùng script đăng nhập của mình để tìm kiếm file chạy Skype.exe; hoặc dùng một script và thực thi nó trên lược đồ địa chỉ IP, gán cho từng client với tài khoản admin phù hợp, tìm kiếm Skype và bất kỳ thiết lập XML hay registry nào tồn tại. Và, tất nhiên bạn cũng có thể dùng một ứng dụng quản lý cấu hình như đã đề cập đến ở trên, hoặc dùng kết hợp cả script với ứng dụng quản lý cấu hình, tùy thuộc xem bạn cần gì, ghi lại, quản lý, ngăn chặn hay xóa Skype.

Loại bỏ Skype

Nếu bạn quyết định cấm Skype lưu hành trên mạng của mình, bạn có thể thực hiện theo một số cách. Đơn giản nhất là “lùng sục” và xóa mọi bản sao của Skype trên từng máy trong mạng. Bạn sẽ cần một công cụ GUI để tìm kiếm và phá hủy Skype. Tiện ích miễn phí có tên SkypeKiller cho phép bạn duyệt mạng, ghi lại danh sách các máy dùng Skype và sau đó xóa chúng từ các máy đó. SkypeKiller cũng cho phép bạn sắp xếp chương trình xóa. Với các máy hiện tại không online, nó sẽ thực hiện công việc của mình tự động ở lần sau, khi các máy đó vào mạng.

Bạn muốn chắc chắn rằng người dùng không thể download và cài đặt Skype, hãy sử dụng công cụ quản lý mạng để loại bỏ truy cập mạng tới website www.skype.com. Vẫn chưa đủ, bởi vì người dùng luôn có thể lấy được phần mềm này ở bất kỳ đâu. Hãy ngăn chặn Skype cài đặt trên hệ thống bằng các tùy chọn Group Policy Active Directory hoặc loại bỏ đặc quyền quản trị người dùng. Bạn cũng có thể dùng ứng dụng quản lý cấu hình để loại bỏ Skype và ghi lại khi Skype được tìm thấy trong quá trình rà soát liệt kê.

Ngoài ra, bạn có thể chạy chương trình kiểm tra khi người dùng đăng nhập hoặc sử dụng các script để tìm kiếm và xóa Skype. Bạn có thể download và sử dụng script `Skype_Delete for Windows` trên website [Web site](#).

Người dùng từ xa là thách thức lớn nhất đối với các quản trị viên, vì họ không kết nối tới mạng cục bộ theo nguyên tắc thông thường. Vậy, quản lý người dùng từ xa hay xóa Skype trên máy của họ như thế nào?

Nếu bạn có một ứng dụng quản lý cấu hình, hãy dùng nó với tác nhân “điện thoại gia đình” khi máy tính được kết nối với mạng riêng ảo (VPN). Sau đó sử dụng các chức năng VPN quarantine (cách ly).

Có thể bạn muốn chờ sau khi người dùng đăng nhập vào mạng cục bộ mới sử dụng một script login để “tóm cổ” họ. Nhưng có nhiều người dùng sử dụng laptop, và hiếm khi kết nối vào mạng cục bộ. Muốn giải quyết vấn đề này, bạn có thể thêm Skype vào chính sách đăng nhập mạng riêng ảo để xác định xem liệu Skype có được dùng hay không. Sau đó xóa chúng khi người dùng đăng nhập vào mạng VPN trong quá trình kiểm tra tường lửa cá nhân và phần mềm anti-virus của họ.

Loại bỏ Skype với Windows XP firewall (Service Pack 2)

Nếu bạn đang dùng Windows XP Service Pack 2 và Windows firewall, có một tiện ích Microsoft cung cấp để điều khiển tường lửa gọi là netsh. Bạn có thể sử dụng lệnh netsh để loại bỏ Skype từ danh sách ứng dụng được cung cấp, hoặc thay đổi quy tắc để Skype sử dụng một địa chỉ IP giả. Thực hiện như sau:

```
netsh firewall set allowedprogram C:\progra~1\Skype\phone\skype.exe Skype disable
```

```
netsh firewall set allowedprogram C:\progra~1\Skype\phone\skype.exe Skype enable custom  
10.1.2.3
```

Loại bỏ Skype ở tầng mạng

Đến bây giờ, chúng ta mới thảo luận về loại bỏ hay xóa Skype trên lớp client. Nhưng thực tế đòi hỏi nhiều giải pháp tổng hợp hơn cho các tập đoàn và công ty lớn cần độ bảo mật cao. Một trong số đó là ứng dụng loại bỏ IM và Skype lớp mạng. Các ứng dụng phần cứng này được cấu hình để nhận diện giao thức cụ thể dùng cho các chương trình như Skype, sau đó loại bỏ lưu lượng mạng của chúng. Những phần mềm như vậy khá đắt tiền, do đó không phù hợp cho các doanh nghiệp nhỏ. Một số trong đó là Verso, Ipoque, Lynanda, SonicWall, Packeteer...

Nếu bạn đang dùng một proxy server như Squid cho tất cả các truy cập Web, bạn có thể cấu hình proxy này để loại bỏ các yêu cầu liên quan đến Skype và IM. Chỉ cần tìm trên Google với từ khóa "Skype AND Squid", bạn sẽ có hàng loạt thông tin về nó.

Quản lý các thiết lập Skype

Chuyện gì sẽ xảy ra nếu bạn quyết định cho phép người dùng sử dụng Skype, nhưng muốn quản lý các thiết lập trên tất cả PC trong mạng? Bạn có thể dùng Active Directory Group Policy hoặc một ứng dụng quản lý cấu hình hay các script như một số ví dụ mẫu tôi đã nói ở trên. Bạn có thể điều khiển hoạt động của Skype như ngăn chặn hệ thống trở thành siêu nút (Supernode), ngắt bỏ quá trình truyền tải file, điều khiển cổng nào và giao thức nào Skype được dùng và một số thiết lập khác. Nếu muốn có danh sách hoàn chỉnh các thiết lập trên Skype, bạn có thể xem tại Skype's Guide for Network Admins.

Cuối cùng, nếu bạn muốn giám sát Skype trên các hệ thống người dùng, sử dụng script đăng nhập Windows để chạy chương trình kiểm tra khi người dùng đăng nhập hệ thống, hoặc chạy "Run Key" trên laptop và ghi lại những gì bạn đang tìm kiếm.