"GIẢI PHẪU" VÀ "ĐIỀU TRỊ" WORM XROBOTS PHÁT TÁN QUA YM

Sau khi nhiều thông tin liên tục xuất hiện về một loại worm lây lan qua chương trình Yahoo! Messenger trong cộng đồng người sử dụng máy tính Việt Nam, nhằm mục đích lây nhiễm các máy tính thành một hệ thống botnet phục vụ ý đồ xấu, một đơn vị nghiên c

Sau khi nhiều thông tin liên tục xuất hiện về một loại worm lây lan qua chương trình Yahoo! Messenger trong cộng đồng người sử dụng máy tính Việt Nam, nhằm mục đích lây nhiễm các máy tính thành một hệ thống botnet phục vụ ý đồ xấu, một đơn vị nghiên cứu bảo mật đã phân tích làm rõ hơn về bản chất con worm (sâu máy tính) này.

Chương trình diệt worm Xrobots

Để diệt worm Xrobots trong các máy tính bị nhiễm, bạn có thể download phần mềm Xrobots Remover (được viết ra ngay sau khi worm này xuất hiện) về máy tính và chạy để chương trình tự động tìm và diệt worm Xrobots, chỉnh lại các registry đã bị sâu máy tính này sửa đổi.

Từ 1g sáng ngày 11-4, tên miền http://xrobots.net đã bị chặn lại để hạn chế khả năng phát tán của loại sâu YM này. Tuy nhiên, các máy tính đã bị nhiễm XRobots có thể bị tác giả sử dụng để cấy thêm các loại virus, spyware, trojan mới vào, nên việc loại bỏ XRobots ra khỏi máy tính cần thực hiện càng nhanh càng tốt.

Tuy nhiên, do hiện chưa có chứng cứ cụ thể, nên đơn vị nghiên cứu bảo mật đã thực hiện việc "giải phẫu" con worm này đã lấy tên gọi của nó là XRobots (tên miền chứa sâu và được sử dụng để phát tán). Sau đây là đánh giá của chuyên gia Nguyễn Phố Sơn, người trực tiếp "mổ xẻ" worm XRobots.

1. Đây không phải là virus. Nó không có tính năng lây nhiễm vào các file, mà chỉ đơn thuần là một loại worm phát tán thông qua trình Yahoo! Messenger. Tạm đặt tên là Worm XRobot.

2. Worm XRobot là tự code sử dụng AutoIt 3, một chương trình "freeware BASIC-like scripting language designed for automating the Windows GUI", dùng để sinh ra mã từ các kịch bản hành vi của user như keystroke, mouse. Worm sử dụng công cụ này nhằm đơn giản hóa việc lập trình, không phải là copy mã nguồn rồi sửa lại như nhận định sơ bộ của một trung tâm tên 911. Tham khảo tại: http://www.autoitscript.com/autoit3/docs/

I. Phân tích hành vi lây nhiễm

1. Thay đổi key:

[HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache] thành giá trị C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files với thư mục Windows cài trên ổ C

Mục đích: thay đổi thư mục mặc định chứa file cập nhật Robots.exe sau khi lây nhiễm

2. Thay đổi các giá trị sau trong registry:

Giá trị ban đầu
Giá trị mới

[HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\Directory]

"C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5"

[HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\Path1\CachePath]
"C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\Cache1"

[HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\Path2\CachePath

"C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\Cache2"

[HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\Path3\CachePath]

"C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\Cache3"

[HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\Path4\CachePath]

"C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\Cache4"

Mục đích: đặt cache mới cho IE

3. Tăng giá trị của internet cache lên 0x137FE

[HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Pathx\CacheLimit]

Với x là 1,2,3,4

Mục đích: gia tăng kích thước cache để chưa file Robots.exe và những thứ khác về sau

4. Chuyển thư mục Cookies, History, Common AppData bằng cách thay đổi các Registry key sau:

[HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies]

[HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History][HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Commom AppData][HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData]

5. Tắt tính năng duyệt offline, bắt buộc user fải duyệt online bằng cách thay registry key:

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\GlobalUserOffline] thành 0x0.

6. Thay đổi và ép buộc sử dụng cấu hình do worm tạo ra, chứ không sử dụng cấu hình mặc định cho kết nối bằng cách thay đổi registry key:

[HKCU\Software\Microsoft\windows\CurrentVersion\Internet ettings\Connections\SavedLegacySettings]

7. Tạo file Messenger.exe tự động chạy khi Win khởi động bằng cách tạo registry key:

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Yahoo!!!]

Có giá trị:

"C:\WINDOWS\Messenger.exe"

8. Thay đổi trang Startpage của Internet Explorer:

[HKCU\SOFTWARE\microsoft\Internet Explorer\Main\Start Page] thành "http://67.15.40.2/~tranphu/forumtp/"

Thông tin có được từ quá trình giải phẫu sâu XRobot.

9. Thay đổi nội dung các registry của Yahoo! Messenger, để khi user bị nhiễm worm, YM sẽ tự động duyệt trang được cài cắm sẵn trên mạng:

[HKCU\Software\Yahoo\pager\View\YMSGR_Launchcast\content url] thành "http://xRobots.net/Gift/New/"

[HKCU\Software\Yahoo\pager\View\YMSGR_buzz\content url]

10. Vô hiệu hóa các công cụ edit Registry bằng cách thêm registry key sau:

[HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools] Có giá trị 0x1

11. Liên tục update worm, tự nâng cấp bằng cách download bản update từ http://xrobots.net/Gift/Robots.exe và chứa trong cache: C:\Documents and

Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\1DELGLE8\Robots[1].exe.
File Robots.exe sau khi được download về sẽ được worm tự động update, ghi lại vào file :\Windows\Messenger.exe. Như đã nói ở trên, file Messenger.exe sẽ tự động chạy khi khởi động Windows.
13. Xóa file %windir%\pchealth\helpctr\binaries\msconfig.exe và sửa đổi file này, chuyển vào thành %windir%\msconfig.exe. Do đó, khi người sử dụng chạy msconfig sẽ không thấy file messenger.exe của worm trong tùy chọn Startup nữa.
II. Cách diệt
* Diệt bằng tay:
1 - Kích hoạt trở lại registry: Download file http://securityresponse.symantec.com/avcenter/UnHookExec.inf. Click chuột phải vào file, chọn Install
2 - Vào Start > Run. Chạy regedit.
3 – Xóa khả năng tự động chạy khi khởi động máy [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Yahoo!!!]
4 – Xóa file chính %windir%\Messenger.exe
5 – Xóa thư mục chứa file update
C:\Documents and Settings\[tên_Windows_user]\Local Settings\Temporary Internet Files\Content.IE5\1DELGLE8\Robots[1].exe.
6 - Copy file msconfig.exe từ máy chưa bị nhiễm vào thư mục:
%windir%\pchealth\helpctr\binaries\
* Dùng công cụ Xrobots Remover:
1 – Download chương trình Xrobots Remover về máy tính của bạn và chạy để chương trình tự động tìm và diệt worm Xrobots, chỉnh lại các registry đã bị sâu máy tính này sửa đổi.
2 – Chạy chương trình và làm theo các hướng dẫn
III. Một số nhận xét và khuyến nghị
- Đây là một con worm rất kém về phương diện kỹ thuật, hầu như chỉ đánh vào số đông người dùng không có ý thức và hiểu biết gì về internet để có thể lây nhiễm. Tuy nhiên, xét về ý đồ của hành vi thì thật sự là một vấn đề cần quan tâm. Lần đầu tiên một con Worm "thô sơ"của người Việt tạo ra đã lây nhiễm manh vào hệ thống mạng máy tính của Việt Nam với một ý đồ hết sức nguy hiểm!
- Rất cần có sự điều phối đồng bộ ở cấp quốc gia trong việc truy lùng tông tích và khống chế các mối nguy tương tự trong tương lai (hoàn toàn có thể thực hiện được về phương diện kỹ thuật).
- Một vấn đề khác cũng cần phải xem xét, đó là trách nhiệm đối với cộng đồng của những đơn vị phụ trách vấn đề phòng chống virus của Việt Nam trong việc phản ứng quá chậm chạp trước một con worm "thô sơ" made in Vietnam như xRobots.
- Nhiệm vụ chính của Xrobot là hình thành mạng lưới botnet, tức là chuẩn bị cho việc cập nhật nội dung chính bản thân nó từ file http:// xrobots.net/Gift/Robots.exe tuỳ theo tác giả mong muốn, worm này sẽ cài spyware, DDOS client, virus khác… lên máy của nạn nhân.
- Các ISP cần có những hình thức phản ứng sự cố tức thời, block website phát tán worm xrobots.net, ngăn chặn việc update của loại worm này.
NGUYỄN PHỐ SƠN (aka Thug4Lif3)