IOWA STATE UNIVERSITY
IT Services Technical Notes

IT

Windows Administrators Meeting

April 10, 2009
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements (None)

W32.Tidserv.G Worm on Campus – Wayne Hauber [ITSEC]

Wayne Hauber [ITSSEC] talked about the latest worm to be affecting a lot of computers on campus. The worm has various names (depending on the AV notification team). W32.Tidserv.G is Symantec's term:
http://www.symantec.com/security_response/writeup.jsp?docid=2009-032211-2952-99

This worm has been seen on both campus-proper and Residence Hall systems. It seems to cause much more problems on Residence Hall systems because the worm brings up a DHCP router based on the switch address it detects on the network. See (again from Symantec):
http://www.symantec.com/security_response/writeup.jsp?docid=2009-032211-2952-99&tabid=2
where it states:

> "The worm modifies the DNS entries on the compromised computer. In case of an infection in a Server/Client environment, clients on a compromised network might acquire malicious DNS addresses from an infected server (without actually being infected itself), redirecting queries to an address controlled by the remote attacker.
>
> The worm acts as a DHCP server for all computers on the compromised computer's LAN, serving the following malicious DNS addresses to redirect all DNS queries to an address controlled by the remote attacker:
> 64.86.133.51 (primary)
> 63.243.173.162 (secondary)
>
> The worm may also download potentially malicious files on to the compromised computer."

For Residence Hall systems this is a "10.10.*" address that cannot get routed further, so the system served by the rogue DHCP server has network trouble. Since campus-proper systems have 129.186.* switches the worm serves out routable DHCP addresses and the effects are less visible. This worm is apparently the product of a group of attackers operating as a team. Wayne said that some systems he has seen have been having web-pages re-directed to blocks of IP addresses in Latvia. It is unknown as to whether or not current anti-virus DAT files protect against this worm. ITS has submitted several samples to the AV community, but it appears the worm authors are very good at having the worm mutate to avoid detection. Using "least priv necessary" while reading mail or browsing the web (the "Windows Vista" model) appears to be a good line of defense (as long as you pay attention to the authorization warnings and don't click "Yes" to everything).

Stephanie Bridges commented they she had seen this worm affect Blackberry devices in her area (probably because of the DHCP damage effects).

It was proposed by someone that 1) user education 2) software to sandbox the web browser and 3) static IP numbers could be a solution. Everyone agreed education was good – but many people won't take the time or the advice given. Software to sandbox the browser is good – but the best ones cost money and still require the user to "think before clicking Yes". Static IPs are running out on campus and not a good general solution to this problem. As always, high security usually requires effort and leads to less user-friendly systems. However, the hackers keep getting better and more malicious.

Thunderbird and POP Mail – Beata Pruski [ITSYS]

Beata Pruski [ITSYS] talked about using Thunderbird with the ITS POP3 mail servers. ITS has some FAQ documentation dealing with setting up Thunderbird as follows:

Windows: http://www.it.iastate.edu/faq/view.php?id=564
Macintosh: http://www.it.iastate.edu/faq/view.php?id=796

ITS has stopped distributing Eudora Pro as a "current" software kit and has effectively withdrawn formal support for Eudora Pro in the Solution Center (mainly because Eudora Pro is no longer supported by the manufacturer).

A large number of email/calendar-related support questions followed:

- The question was asked as to whether there would be added support on the existing POP3 mail servers to handle SSL connections. John Hascall [ITSYS] responded that the upcoming "Gmail" (Google) project and expansion of the Microsoft Exchange services are the likely future email services on campus. POP3 is simply not the way to move forward.
- Vince Oliver [ITSYS] stated that ITS may support secure IMAP on the Exchange system – but not POP3.
- General comments were made that calendaring was supported on both Gmail and Exchange (lacking on POP3).
- Stephanie Bridges [ECONA] commented that the Lighting calendar extension for Thunderbird worked well with Gmail.
- Jim Wellman [A ERE] commented that migration of large mailbox stores from one mail system to another (Eudora to Thunderbird?) can be a problem unless they are broken up into smaller pieces.
- Someone indicated a technique they used successfully to migrate Eudora mail to Exchange was to use the IMAP mail store on both systems.

- Wayne Hauber [ITSEC] asked if anyone was experimenting with a “Eudora Template” for Thunderbird (nobody was).

Open Discussion

Ted Peterson [STAT] asked if anyone else had dealt with Windows XP systems that keep attempting to reinstall the same update. Mike Lohrbach [ITSYS] said he had see XP SP3 fix such problems on one systems. Other people commented that sometimes a “corrupted update cache” would cause this. Here is a good Microsoft article on how to manually clear a corrupted cache if you want to try this: http://support.microsoft.com/kb/958046

Meeting Adjourned (9:55)

Next meeting is scheduled for May 8.