What's Next ?

Alexandru BĂLAN
<abalan@bitdefender.com>

Short Summary

- Last year...
  - Types of malware
  - Should AV producers take care of Linux boxes as well ?
- Now...
  - More threats
  - More defenses
- What's next ?

Last year we talked about...

- Examples of malware (viruses, rootkits, exploits, social engineering)
- Windows people having all the “fun”
- Apparently there's no need right now for AV producers to extend their focus to *NIX firewalls, rootkits and so on.

However

- The industry is shifting from protecting the data to protecting the information
- If companies have any number of employees at all, studies show and human nature shows that there's always going to be be somebody that is going to try and take advantage of the system
- New threats are emerging

Now..

- More threats (not necessarily new)
  - Botnets
  - Code running on your computer (client side javascript)
  - Tons of php/sql_injection/other exploits.
  - The human factor is (as expected) an increasing risk

What do you see as tomorrow's threats and defenses ?

Examples:

- Cisco/IOS rootkit
  - Presented at EUSecWest London UK – May 2008
  - Just “an interesting concept ?”

  Sebastian Muniz: I've been told by the cousin of a friend of my girlfriend that this kind of rootkit has previously been used :)

Source: http://eusecwest.com/sebastian-muniz-da-ios-rootkit.html

What do you see as tomorrow's threats and defenses ?

- Web OS – It's going to happen!
- Threats from and through social networks (read: facebook, myspace, ect, ect) are just an example:
  - It's not exactly spam and it's not exactly phishing. You can't even call it “tricking the user”. The users are ignorant enough to click everything and get in contact with everyone
  - *5 out of 10 “add me” requests are approved on IM*
  - *7 out of 10 “add me” requests are approved in SNS*
  - *Usually comments are on a “accept all” basis*

What do you see as tomorrow's threats and defenses ?

- Phlashing – Remote DOS in any device that supports firmware update
  - Attacking system firmware isn't a new tactic—the CIH/Chernobyl virus was capable of overwriting BIOS firmware back in 1998—but focusing such attacks on network hardware would be an unusual step, and could prove quite successful in at least the short term.

Source: http://arstechnica.com/news.ars/post/20080520-phlashing-attacks-could-render-network-hardware-useless.html

What do you see as tomorrow's threats and defenses ?

- “14-Year-Old Turns Tram System Into Personal Train Set”
  - A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents.
  - The 14-year-old modified a TV remote control so that it could be used to change track points

Source : http://www.theregister.co.uk/2008/01/11/tram_hack/

What do you see as tomorrow's threats and defenses ?

- Firewire DMA bug (connect a laptop to a firewire port, trick the machine into allowing you read/write memory access)
  - A tool targeting mainly Windows XP systems has been released by Adam Boileau
  - To use the tool, hackers must connect a Linux-based computer to a Firewire port on the target machine. The machine is then tricked into allowing the attacking computer to have read and write access to its memory.

Source: http://www.theage.com.au/news/security/hack-into-a-windows-pc-no-password-needed/2008/03/04/1204402423638.html

The conclusion

- Innovation and allocating resources to develop a solution for a future threat (i.e. cisco anti-rootkit) is risky.
- Awareness is still low and surprisingly, getting lower. 10/10 random people asked, will not bother with security for “exotic” threats.
- Leaks from the underground have been plugged. We haven't heard about anything tasty in some years. This silence is a bad sign

The conclusion (cont)

Because of the above, it's difficult to predict and develop the security solution for tomorrow and it's increasingly easy for attackers to predict where and how to strike next.

What can YOU do

- Share information !
- Demand more from the industry. No matter how crazy it might sound today it might just be something we won't be able to live without tomorrow
- Don't be afraid to “waste resources” with innovation.
- Let us know. Send your requests and thoughts toabalan@bitdefender.com . My spam filters as well as our research teams will be happy to take note of them

Q & A