Malware

Steve Romig
April, 2006

Agenda

- Interesting stats
- Rootkits
- Botnets
- Q&A

Interesting Stats

- 90% of our compromised machines are bots
- Most of these are *not* detected by anti-virus (not running, not up to date, not found)
- Most cannot be disinfected easily (rebuild!)
- Most are not detected through “usual” means - scanning, ddos, outside reports...
- Hard to spot, but common

Interesting Stats

- Kaspersky's 2005 Malware Evolution, part 2:
- Cybercrime makes more $$ than security
- (Others say fraud is more $$ than drugs)
- 76% of people don't update anti-virus daily
- 45% open suspicious email at least some of the time
- Kaspersky provides HOURLY updates

Interesting Stats

- Microsoft's Anti-malware Engineering Team:
- Malicious software removal tool runs on 250,000,000 computers/month
- 250,000 computers infected with Alcan (p2p spreading worm)
- No SP: 50% have rootkit
- SP1, SP2: 20% have rootkit

Rootkits

- The Holy Father and Hacker Defender
- U of M, Microsoft and SubVirt
- Joanna Rutkowska - cross-view detection and Stealth by Design

Botnets

- What they are
- What they are used for
- How they spread
- How to detect them

What is a Botnet?

- A “bot” is a software agent that miscreants install on your computer to make it part of a botnet.
- A “botnet” is a network of bot infected machines. The bots talk to each other, frequently through IRC (Internet Relay Chat).

What is a Botnet?

- The owner (aka bot herder) can send commands to the bots through the botnet.

What Are They Used For?

- Sending spam, facilitate phishing
- Installing spyware/adware
- Keystroke logging (passwords, credit cards...)
- Building botnets
- Denial of Service
- Click fraud

How Do They Spread?

- Mostly social engineering, through IM, email, peer-to-peer file sharing
- Remember those stats?
- LOL - not a virus! (MySpace)

How to Detect

- Yow, its hard
- Detect commands (snort rules)
- Evaluate C&C servers
- Check flows for connections to C&C
- Secret Squirrel
- Botnets mailing list

Example

- 17:05 -!- Topic for #jordan23: .aimspread look at this sad killing
- http://www.freewebs.com/omgsadkilling/killed.com
- 17:05 -!- Topic set by Rob- [] [Fri Apr 7 13:33:48 2006]

Rebuild!

- People are resistant to this
- Its hard to disinfect a machine when you don’t know what’s been done to it
- Microsoft even admits now that rebuilding is usually best

One Last Thing

- Kernel mode rootkit/bot by tibbar
- Everyone's talking about infecting the BIOS or video memory or...

References

- Microsoft anti-malware engineering team blog: http://blogs.technet.com/antimalware/
- Kaspersky: http://www.viruslist.com/en/analysis
- Tibbar: http://tibbar.blog.co.uk
- Joanna Rutkowska: http://invisiblethings.org