Effective Malware: The Importance of Stealth

Henry Stern

Senior Security Researcher

Cisco IronPort Systems LLC

The Conflict of Stealth and Interest

Boring is Beautiful

- Be malicious.
- Be boring.
- Be succesful.

What is Interest?

- Malware needs to do something.
- Doing something causes interest.
  - Noisy.
  - Destructive.
  - High tech.
- Sufficient interest provokes action.

What is Stealth?

- Evading interest.
- Malware is more effective when not countered.
- Countering malware costs resources.
- Malware is tolerated if it is not interesting.

The State of Practice

- We tolerate certain levels of malfeasance.
- Attackers are not always observant of this.

  e.g. Conficker vs. Gh0stNet
- Maybe they should be!

The Bestiary

- Imbot
- ASProx
- Conficker
- Storm (Waledac)
- Reactor Mailer 3 (Srizbi)
- GhostNet

IMbot

- Malware: Imbot.AC, Bifrose.E.
- Infection vector: Instant Messenger.
- Size: 50k sustained.

  15k new bots per campaign.

  Roughly same cleaned up.
- Exploits trust between IM friends.
- Social pressure to clean infections.

  "Hey, you have a virus and it's spamming me."
- Large amount of effort required to sustain bot pool.

ASProx

- Behaviour: Mass SQL injection.
  - Javascript payload.
- Generic MSSQL function infects all fields in table.
- Large number of compromised websites for first layer of javascript redirection.
- Small number of hosts for actual exploit code.
- Too many sites infected to clean up.
- Involves enough third parties that clean-up is effectively impossible.

Storm (Waledac)

- Purpose: Spam, DDOS.
- Infection vector: Social engineering, now Conficker.
- Infamous for its social engineering campaigns, peer-to-peer rendezvous protocol, fast flux service network.
- Spam activity was low and slow.
- Attracted too much attention, was never especially effective at spamming.
- Poorly-implemented, high tech features resulted in total subversion.

Conficker

- Behaviour: Scanning worm.
- Purpose: Vehicle for secondary infections.
- Infection vector: MS08-067 buffer overflow.
- Size: Millions.
- Technical sophistication attracted significant researcher, media attention.
- Enormous development investment from malware authors.

Reactor Mailer 3

- Malware: Srizbi.
- Size: 260k+ bots.
- Responsible for more spam than all other botnets combined.
- Infection vector: Browser exploits, social engineering.
- Purpose-built spam tool. No other functionality.
- Full-kernel rootkit, minimal user disruption.
- Trivial for security vendors to block symptoms.
- Survived 18 months without major harassment.

GhostNet

- Malware: gh0st RAT.
- Infection vector: Targeted social engineering.
    - Specific, known groups and individuals.
    - High degree of human intervention by attacker.
- Dates back as far as 2002.
- Accusations of foreign government involvement.

A Taxonomy of Interest

The Taxonomy

- I am infected.
- My friend is attacking me.
- Somebody around me is infected.
- Somebody is attacking me.
- Something nearby is shiny.

I am Infected

- Do I notice anything?
- Does it adversely affect me?
- Is it important enough for me to act?

My friend is attacking me.

- Is it something I see?
- Does it harm me or my other friends?
- Is it worthwhile for me to act?

Somebody around me is infected.

- Is it affecting my usage of a shared resource?
- Will it go away on its own?
- Will my actions be effective?

Somebody is attacking me.

- How much damage is being done?
- Can I do anything about it?
- Will it happen again?

Something nearby is shiny.

- Is it kewl?
- Is it newsworthy?
- Is it understood?

Implications

Common Failings

- Malware is too exciting.
- Indiscriminate attacks.
- Excessive population sizes and activity.
- Whiz-bang features.

Why Not Boring?

- Tip-toe around users, avoid their friends.
- Low-volume, focused attacks.
- Don’t be shiny.
- Clean up afterwards.

Are They Already Boring?

- Sophos estimated 11m unique samples in mid-2008.
- Collins estimates that 10% of flows are definitive mysteries.
- What’s in the long tail?