Spam/Malware

John Roy 5/31/12

Definitions

- Malware
  - software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to a computer system
- Spyware
  - collects information about users without their knowledge
- Spam
  - Unsolicited bulk electronic messages typically hawking unscrupulous products

Typical Toxic Email

This message was marked as spam using the Outlook Junk E-mail filter.

From: [redacted]
Sent: Tue 5/29/2012 3:56 PM
To:
Cc:
Subject: HI

wow give this a look http://www.dorenews.net/biz/?employment=0833914

This message was marked as spam using the Outlook Junk E-mail filter.

From: [redacted]
Sent: Mon 5/28/2012 2:55 AM
To:
Cc:
Subject: Hey

this is pretty intense you should give it a look http://www.news15de.net/biz/?page=2809532

What Do You Do?

- **Delete, Delete, Delete**
- Are you Cautious or Curious?
- Never click on any suspicious email even if it is from someone you know.

Compromised Email Categories

- Your Computer is Infected
- Your Email Address has been Hacked
- A friend's computer with your email address has been compromised
- Your email address has been spoofed

Your Computer is Infected

- Antivirus Software will not protect you from opening an infected email
- Antivirus Software may or may not detect what was propagated into your computer by opening an infected email
- You need to run ancillary Malware utilities such as Malwarebytes, Spybot Search & Destroy, etc.
- **Note:**
  - These utilities are in addition to anti-virus software. They should be run periodically. It's best to use more than one malware utility.

Your Email Address has been Hacked

- Contact your ISP
  - This may be difficult if using a free account
- Change your password
- Create a new Email Account
  - If you don't have access to your email account then it probably was hacked
  - Use the "I forgot my password" link to see if you can gain control and change your password

Another Computer (with your email address) has been Compromised

- Much more difficult to track back to the person that has your email in their address book
- If you get enough clues to determine who may be infected then they need to take the actions outlined for your personal computer

Your Email Address has been Spoofed

- The sender information shown in the "From" field has been changed. Spammers do this to hide the origin of their e-mails. It leads to problems such as misdirected bounces
- Address spoofing is like writing a forged return address using snail mail. As long as the letter fits the protocol, (i.e. stamp, postal code) the SMTP protocol will send the message.
- No Easy Solution for this
- Wait it out and hope it subsides or take actions previously outlined like closing your account and opening a new one.

Avoid Questionable Email

- Be Cautious **NOT** Curious
- **Delete, Delete, Delete**
  - Better to delete a suspicious email than to open it
  - Your friend can always resend a legitimate email
- Never Respond or Opt-Out

Notifying Known Sender

- If the questionable email came from a known sender you can advise that person of the hijacked email.
- Send a new email to known sender about the hijack
- Attach a Graphic of the Email Received
  - Ensures toxic link is not inadvertently clicked on

Malware Software (Free)

- Malwarebytes
  - Free & Paid ($25)
  - http://www.malwarebytes.org
- Spybot Search & Destroy
  - Free, donations accepted
  - http://www.safer-networking.org/en/download/
  - **CAUTION:** Do Not download "Spybot" it is a known worm
- Windows Defender
  - Free
  - http://www.microsoft.com/en-us/download/details.aspx?id=17

Malware Software (Free) Continued

- SuperAntispyware
  - Free & Paid ($30)(Live CD available $15)
  - http://www.superantispyware.com/download.html
- Ad Aware
  - Free & Paid ($30)
  - http://www.lavasoft.com/products/ad_aware_free.php
- Combo Fix
  - Free but not advised for novice

Other Malware Software ($$)

- Spyhunter ($40+)
- Spyware Doctor ($30)
- Stopzilla ($40+)
- Spysweeper ($40)

Hijackthis

- Scans computer, displays browser hijacking locations
- Does **NOT** remove or detect spyware, adware
- Generates a plain text log file detailing all entries it finds.
- Advanced users can use to remove unwanted settings/files or obtain free help here
  - http://hijackthis.de/index.php?langselect=english

Other Portable Utilities

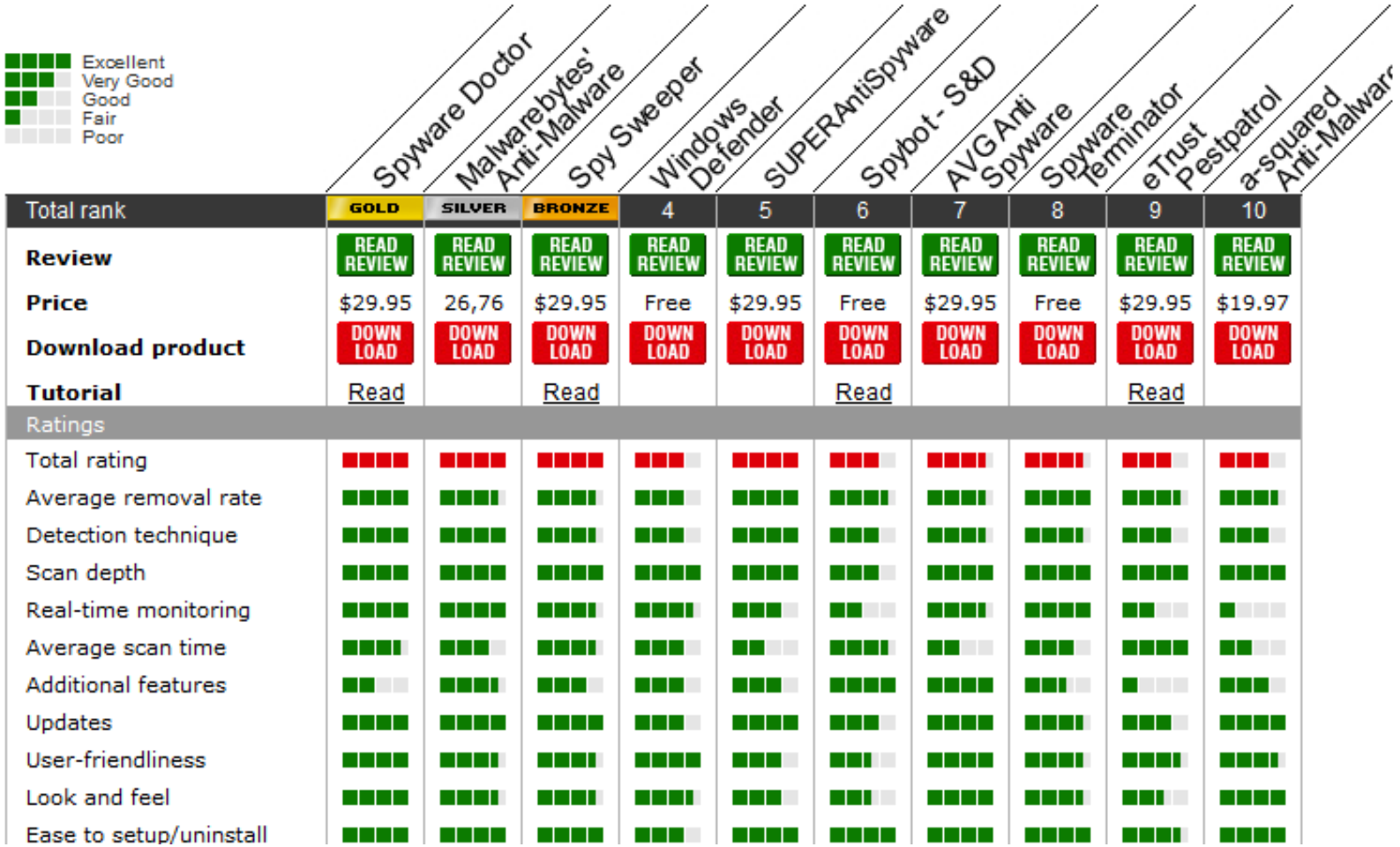
- AVG Rescue Disk (free)
  - www.avg.com/us-en/avg-rescue-cd
  - Download and create a bootable media
  - If connected to Internet S/W will update before scanning
- Windows Defender Offline (free)
  - http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline
  - Download and create a bootable media
- Microsoft Safety Scanner (free)
  - http://www.microsoft.com/security/scanner/en-us/default.aspx

Microsoft Product Confusion

- Microsoft Security Essentials (MSE)
  - Active Real Time scanner
  - For spyware/adware, viruses, worms, some rootkits.
- Windows Defender (P/O Vista & Win7, free D/L WinXP)
  - Part of MSE
  - Only scans for spyware/adware
  - Stand alone portable scanner available (Windows Defender Offline)
- Microsoft Safety Scanner
  - Stand alone portable scanner (expires in 10 days)
  - For spyware/adware, viruses, worms, some rootkits.

Anti Spyware Comparisions

http://www.2-spyware.com/compare.php



Useful Security Information Links

- **Microsoft Safety & Security Center**
- www.microsoft.com/security/default.aspx

- **Security Tips & Talk Blog**
- http://blogs.msdn.com/b/securitytipstalk/

- **Security Garden Blog**
- http://securitygarden.blogspot.com/

Parting Shots

- Protect your email address
- Preferably use a throw away email address when you signup for something at less known websites
- Use Blind Carbon Copy (BCC) to send generic email and train your family and friends to do the same
- When its necessary to publish your email address replace the "@" symbol with "at" to elude Spam web crawlers
- Create account passwords that are difficult to guess

Conclusion

- Be Smart, it's better to delete a real email than to open an infected email

- Questions?