Windows Security and Privacy

Probus

June 2011

Art Hunter

Over 60,000 security attacks were launched per day in 2010, an increase of about 70 per cent over the previous year!

Introduction – Slide 1

Achieving Security in this document means both protection and recovery.

- Access control to the PC - protection
- Destination control of Internet links – protection
- Encryption – data protection
- Recovery after infection – disaster recovery due to any cause
- There are a vast number of programs available. This list is the author's choice of free high quality products. This list will change regularly in pace with the ever expanding threat. URLs have a lifetime, use Google search if these are outdated.
- Network Security and Disaster Recovery is Everyone's problem.

VisualBee

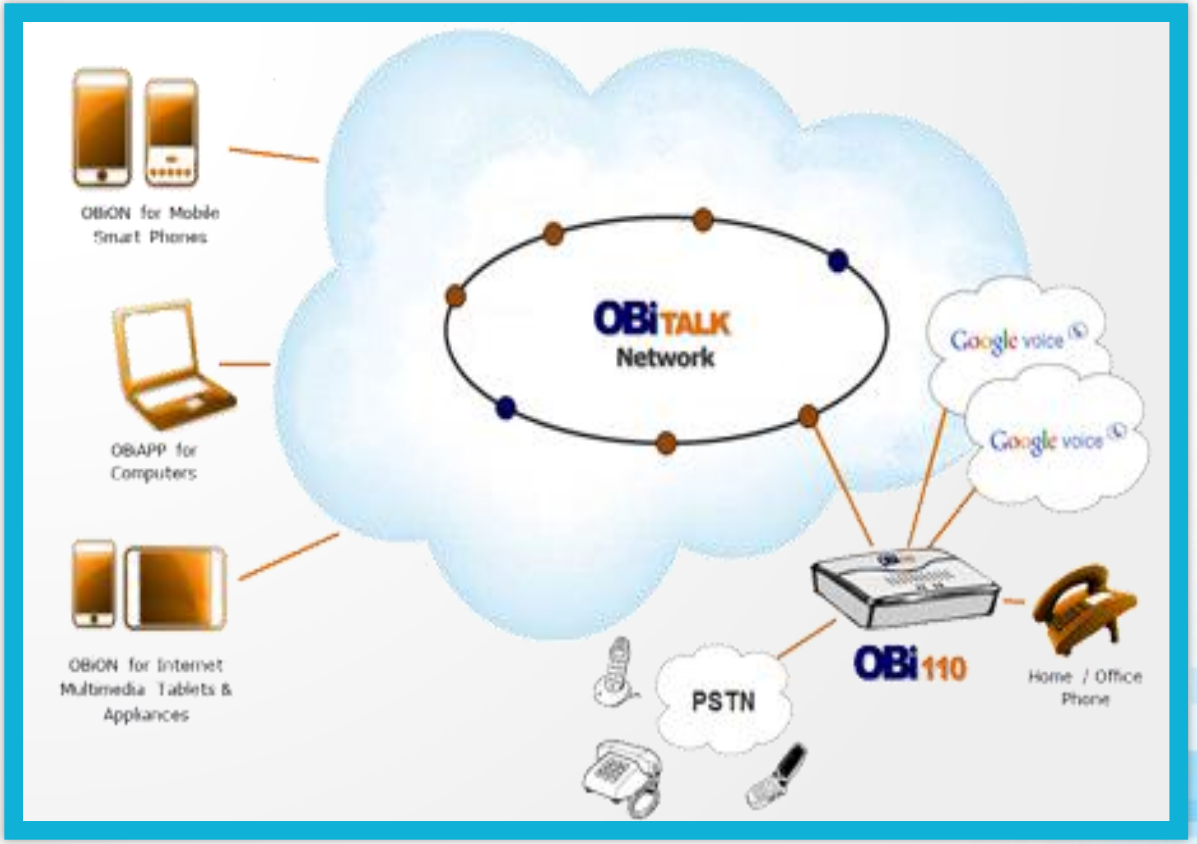
Terminology & Techniques – Slide 2

- Malware – Virus, Keylogger, Trojan, Worm, Backdoor, Spyware, Rootkits
- Zero Day – Just released into the wild
- Drive by Infection – just normal WEB surfing
- Phishing – site spoof encouragement to disclose information
- Spear Phishing – target you or a group
- Social Engineering – Nigerian $ millions spoofs
- Peer-to-peer – direct link between computers
- Botnet – computer hijacked, now a zombie – email addresses

The Cloud – Slide 3

Grow x7 by 2015 – 1.2 zettabytes (1021)– Asia centric and leading**

1,200,000,000,000,000,000,000 bytes



VisualBee

Why Attack me? - Slide 4

Resource control

- DOS – denial of service
- Botnet
- Invite their friends - communications

Data theft – big business

- Banking and financial
- Profile analysis for attack shaping - surveys

Direct Selling

- Scareware & PC hostage (pay me or else)

Four Major Attack Vectors – Slide 5

- Drive by – not your fault (?)
- Exploit vulnerabilities – not your fault (?)
- Social Engineering/Phishing – next slide
- Downloads – e.g. Vuze, Warze, Torrents -- 1/14 infected
- Minor threats
  - Infected email attachments – jpg, pdf, doc, exe, zip, rar, 7z, etc
    - 90% email traffic is SPAM, junk advertising or phishing
  - Thumb drives
  - Shared CD/DVD
- Microsoft - "the company has seen a 1,200-percent increase in the presence of phishing via social networks" in the second half of 2010, versus the first half.

Social Engineering/Phishing Example – Slide 6

- Dear Chase Online[SM] Customer:

  We've detected unusual activity on your account. As a result of this, your Online Banking has been deactivated for Security purpose.
  This has been done to secure your account and to protect your privacy.
  Chase Online[SM] is committed to making sure that your online transactions are secure. We require you to complete an account update to reactivate your online access.

  To start the reactivation process click on Chase Online[SM].

  Once you have completed the process, we will send you an email notifying that your account is available again. After that you can access your account online at any time.

  The information provided will be treated in confidence and stored in our secure database.
  If you fail to provide required information your account will be automatically deleted from Our online database.

  Thank You
  Online Services Team.

VisualBee

Layered Defense – Slide 7

- The PC owner must be aware of the attacker's strategies.
- The PC owner must be aware of the capabilities of their PC system.
- The PC owner must establish and maintain a layered defense against attacks.
- If very sensitive data then don't use a computer that has been or ever will be connected to the Internet. E.g. banks
- Read the features and benefits stated in each of the following URLs.

VisualBee

Priority Security & Privacy Layers – Slide 8

- 1. Firewall -- Access Control (Windows default)
  - http://windows.microsoft.com/en-US/windows7/Understanding-Windows-Firewall-settings (2-way use ZoneAlarm)
- 2. Microsoft Security Essentials – Access Control & Cleaning
  - http://www.microsoft.com/security/pc-security/mse.aspx
- 3. ThreatFire – Behaviour & Access Control
  - http://www.threatfire.com/download/
- 4. OpenDNS – Destination Control (advertisers and criminals)
  - http://www.opendns.com/solutions/overview/
- 5. Immunet Project – Access Control
  - http://www.immunet.com/main/index.html
- 6. WinPatrol – Privacy
  - http://www.winpatrol.com/download.html

VisualBee

Priority Layers (continued) – Slide 9

- 7. Secunia Personal Software Inspector – Access Control - vulnerabilities
  - http://secunia.com/vulnerability_scanning/personal/ 200 software programs on mine
- 8. Belarc Advisor – Privacy and Access Control
  - http://www.belarc.com/free_download.html
- 9. Adobe Flash Player Management Settings – Privacy
  - http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html
- 10. Hosts – Destination Control and Privacy (Like OpenDNS)
  - http://someonewhocares.org/hosts/ and http://www.abelhadigital.com/hostsman
- 11. Delete Pagefile.sys – Privacy (malware mining & forensic evidence)
  - http://support.microsoft.com/kb/314834

Priority Layers (continued) – Slide 10

- 12. Restore Points – Recovery
  - http://windows.microsoft.com/en-US/windows-vista/System-Restore-frequently-asked-questions
- 13A. Easeus Hard Drive Image – Recovery
  - http://www.todo-backup.com/products/home/
- 13B. Windows 7 Emergency Repair (image and restore point boot disk) – routine backup, trial restore
  - http://www.tomstricks.com/how-to-create-a-windows-7-emergency-repair-disk/
- 14. Ten safe Online Scanners – Recovery
  - http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/online-scanner
  - http://www.bitdefender.com/scanner/online/free.html
  - http://housecall.trendmicro.com/
  - http://www.kaspersky.com/virusscanner

Priority Layers (continued) - Slide 11

- 14. (cont) Online Scanners – Recovery (continued)
  - http://www.pandasecurity.com/homeusers/solutions/activescan/
  - http://www.microsoft.com/security/pc-security/malware-removal.aspx
  - http://onecare.live.com/site/en-us/default.htm (from Microsoft)
  - http://www.eset.com/online-scanner
  - http://home.mcafee.com/store/Product.aspx?productid=mss
  - http://cainternetsecurity.net/entscanner/

  Do at least one Online scan of your system so you have that experience available when it comes time when you really need it. Scanning will not hurt your machine when there are no infections present.

Priority Layers (IE 9) - Slide 12

15A. Internet Explorer 9 (Vista and Windows 7 only) – Privacy and Destination Control

- http://windows.microsoft.com/en-US/internet-explorer/downloads/ie-9/worldwide-languages
- Internet Explorer 9 protects against 99 percent of socially engineered malware (augments ZoneAlarm, HOSTS and OpenDNS)
- socially engineered malware describes any link that leads to malicious web sites or downloads that could harm your computer.

VisualBee

Priority Layers (IE9) – Slide 13

- 15B. Internet Explorer 9 (Vista and Windows 7 only) – Privacy using Tracking Protection Lists - TPL
  - http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx (Features explained - profiling)
  - http://ie.microsoft.com/testdrive/Browser/TrackingProtectionLists/Default.html (available lists)
  - http://www.zdnet.com/blog/bott/ie9-and-tracking-protection-microsoft-disrupts-the-online-ad-business/3004?tag=nl.e539 (who can you trust?)

  Do read prior to deployment to avoid undesired effects.

16. VIRUS Total Chromatizer – Slide 14

16. **Vtchromizer is a free extension for use with the Chrome Browser.** Also available for FireFox.

- Find a file you want to download, right click and choose **Scan with VirusTotal**, and wait for the analysis by up to 42 virus scanners to complete.

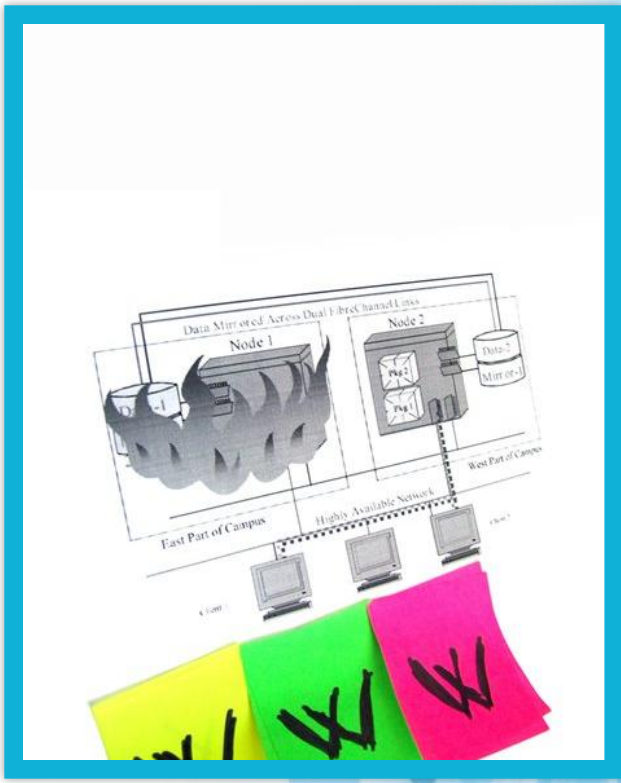
- Find a URL you think is suspicious. Right click the link and let VirusTotal assess it with 13 safe browsing scanners.

https://chrome.google.com/webstore/detail/efbjojhplkelaegfbieplglfidafgoka

VisualBee

17. AVG Link Scanner for Windows – Slide 15

- Checks WEB pages in real time to protect against Drive By attacks (5th layer for destination control)
- Will check danger of links prior to your click
- Free
- http://linkscanner.avg.com/



VisualBee

Miscellaneous Security Practices – Slide 16

18. Strong passwords 1963 --> 9Teen6Tthree You MUST use a windows boot up password for network protection.

19. Use of alternate email addresses for “identification” . They are free and can be tossed away by ignoring them.

20. Beware fake security messages (links into the cloud). Malware Social Engineering takes many forms.

21. When WEBmail compromised by Botnet, change the password.

VisualBee

22. InPrivate Browsing –Slide 17

- Control+Shift+P when in Internet Explorer
- *InPrivate Browsing* helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.
- To turn off InPrivate Browsing, close this browser window.

VisualBee

Preventative Maintenance – Slide 18

- Preventative maintenance and security are strongly linked. Learn how to and use the features of Ccleaner often.
  - Cleaner for windows and applications (privacy)
  - Registry (privacy)
  - Uninstall unused programs (destination control)
  - Startup (privacy)
  - Review Restore Points (recovery)
  - Manage Cookies (privacy)
  - Wipe your free space on your hard drive (privacy)
  - http://download.cnet.com/ccleaner/

System File Checker - Slide 19

Only for advanced users -- recovery option.

Open command prompt with elevated Administrator level

C:> sfc /scannow

Scans for missing or corrupted system files and repairs them

http://support.microsoft.com/kb/929833

All command line commands available at

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntcmds.mspx?mfr=true

VisualBee

Evercookies - Slide 20

New threat in 2010

Tracking cookies that last FOREVER!

They are regenerative in that 8 copies hide on your hard drive. Only one needs to survive a cleaning operation to regenerate the others.

Bleachbit is like CCLEANER on steroids. Both will go after evercookies.

http://bleachbit.sourceforge.net/

Compatibility – Slide 21

All the tools stated in this document operate without adverse interactions on the author's six machines.

Each person is responsible for the security of their computer. Reading, understanding and deploying the security tools on each of the listed URLs is vital to maintaining a high degree of layered PC security.

VisualBee

Some Other Free Tools with an excellent reputation – Slide 22

http://www.bleepingcomputer.com/download/anti-virus/combofix - Recovery but dangerous if other virus scanners present

http://www.malwarebytes.org/mbam.php - virus scanner protection

http://clonezilla.org/ - full image generation and restore

VisualBee

Under Evaluation By Me – Slide 23

- Sandboxie -- installation isolation
- Mozy Home – cloud storage
- Gladnet Cloud Desktop – cloud storage
- Windows Live Skydive -- cloud storage
- VMware Player – virtual PC
- Win7 Virtual XP Pro – virtual PC
- Ubuntu 11.04 – Linux (Mint 11)
- Genie Timeline – real time backup
- UnhackMe -- Rootkit check loading RAM

Common dangerous passwords – Slide 24

http://www.duosecurity.com/docs/top250gawker.txt

- 2516 123456
- 2188 password
- 1205 12345678
- 696 qwerty
- 498 abc123
- 459 12345
- 441 monkey
- 413 111111
- 385 consumer
- 376 letmein
- 351 1234
- 318 dragon
- 307 trustno1
- 303 baseball
- 302 gizmodo
- 300 whatever
- 297 superman
- 276 1234567
- 266 sunshine
- 266 iloveyou

VisualBee

Plan Now For Disater Before It's Too Late

– Slide 25

Security is not "set and forget" but requires maintenance. Much is automatic updating but some is not (e.g. Ccleaner). Become an active participant in your own protection.

The threat changes. New vulnerabilities are found. Malware authors are growing in numbers and power as it is very profitable. PC owners must be aware and then deploy new counter measures against advanced persistent threats.

Over 60,000 security attacks were launched per day in 2010, an increase of about 70 per cent over the previous year!

Closing Comment - Slide 26

- Online privacy/security often comes down to one thing: common sense. Be aware of what you are clicking on. Don't just give away personal information when someone asks. Make sure you know who is asking and why they need to know; when in doubt, just disconnect and think it over — especially when responding at social media sites. For the very nervous techno-novice, call the bank on the telephone and do business on the telephone as the telephone can be more secure than the Internet. For the rest, use security layers.

VisualBee

Windows Security and Privacy

Probus

June 2011

Art Hunter

Over 60,000 security attacks were launched per day in 2010, an increase of about 70 per cent over the previous year!