Now that you have the latest antivirus software, are you truly safe?

Presented by

Michael J. Moore, MBA, MCITP, MCSE, MCSA, MCTS, MCP.

National Cybersecurity Month

Presentation Outline

- Introduction
- Types of Malware
- Other Security Terms
- Methods of Attack
- Other Types of Scams
- Protections Methods
- Statistics
- What should I do?
- Tools and Information
- Works Cited
- Questions

Types of Malware

Malware (Malicious Software): Is a program which accesses a computer system often without the owner's knowledge or consent.

Virus: These are various types of programs that can be memory resident and attaches itself to .com or .exe files, so when these files are executed the virus loads too. Viruses can be run from hard drives, boot sectors, floppies, flash drives or anything else which can store a file. Viruses spread by using a file and replicating this file to other places. Requires some sort of user interaction: Inserting a disk, booting a computer, etc.

- *File*: Infects a file and infects the system when the file is executed.
- *Boot Sector*: These infected the Boot Sector, which is an area on the disk which is read when a computer is started up.
- *Multipartite (Polypartite):* Infects both boot records and program files.
- *Macro:* These use the programming language of the host file to further the infection. Word, Excel and other files which have internal programming language, which is often used to run code to compromise a system.

Types of Malware (Continued)

Polymorphic Virus: This type of virus has the ability to rewrite a portion of itself in order to avoid detection.

Worms: These types of programs can spread from system to system without the use of a host file. (Direct Copy) Worms can exist inside of other files such as a Macro Virus. The main difference between a virus and a worm is a worm requires no user interaction to replicate.

Trojans: Much like the Greek myth of the Trojan Horse, a Trojan is a program which masquerades as something else. It could be an EBay monitoring program, which will monitor EBay auctions, but it is will also do anything else the programmer wanted it to do. It is often software which promises to do one thing, yet this is just a ruse to get the user to execute it.

Types of Malware (Continued)

RootKit: Is a program designed to stay concealed on a system. This type of program can prevent itself from being visible in a system's list of processes, and/or prevent the program files from being read by detection software. This software provides a hacker with a virtually undetectable back door into the host system.

"A RootKit isn't concerned with self-propagating, generating revenue from advertisements or sending out mass quantities of network traffic. RootKits exist to provide sustained covert access to a machine, so that the machine can be remotely controlled and monitored in a manner that is extremely difficult to detect."

-Blunden, R. B. (2009). *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System.* Plano, Tx.: Wordware Publishing, Inc.

Types of Malware
(Continued)

Spyware: It collects information about use and actions of the user and then sends this data to a central repository. Often installed with another piece of software.

Adware: Though this term is not used as much anymore, and it can be classified as harmless, though it can be annoying. It is any software which has an advertising portion added to it and it is used to generate revenue for the owner. Sometimes, this software is bundled with spyware so it can tailor the ads to the user.

Rogueware

» **Rogueware:** This is software designed to mislead the user into believing their workstation is infected with Malware and prompts the user to pay to have it removed.

Types of Malware (Continued)

Keyloggers: Tracks which keys are typed on a keyboard. The various types of keyloggers are:

- *Software:* A software program which records the data from the keyboard controller.
- *Keyboard overlays:* Often used on ATMs or other places a PIN might be used.
- *Acoustic Keyloggers:* A sound profile of a keyboard is generated, and from that sound profile key presses can be determined.
- *Electromagnetic:* Senses the electronic emissions from a wired keyboard as keys are pressed from 20 meters or 66 feet away. (Knight 2000)
- *Surveillance:* Using a concealed camera to determine key press.

Other Security Terms

BotNet: A collection of computers which are programmed to perform a variety of tasks, from Denial of Service (DoS) attacks to sending spam. A 'Bot Herder' is the person who is in remote control of the BotNet, and some rent out their Bots for a fee to various clients.

Exploit Kit: Is software which allows a user to take advantage of known exploits in applications, such as: Internet explorer, Adobe Acrobat, Microsoft Office, etc. These kits are marketed and sold on the premise of revenue generation to the user. These kits are being used to create BotNets for fun and profit!

Zero-Day: These are vulnerabilities in software that are not known to the developer and someone has developed an exploit to take advantage of the flaw.

Other Security Terms (Continued)

Spoofing: Is the technique in which a person or program masquerades as another.

Pharming (Pronounced like *farming*): This is when a hacker redirects a website's traffic to another, fake website. Victim then enters in their credentials thinking it is a trusted site. This can be done via a number of methods: DNS, host file, etc.

Phishing (Pronounced like *fishing*): This is a process of sending out blind emails in an attempt to get someone to click on a link to a website under control of the sender. It is on this website the sender will want the prey to enter personal information or the website could be running an exploit kit.

Spear Phishing: Using targeted email messages with infected links from people the recipient can trust.

Methods of Attack

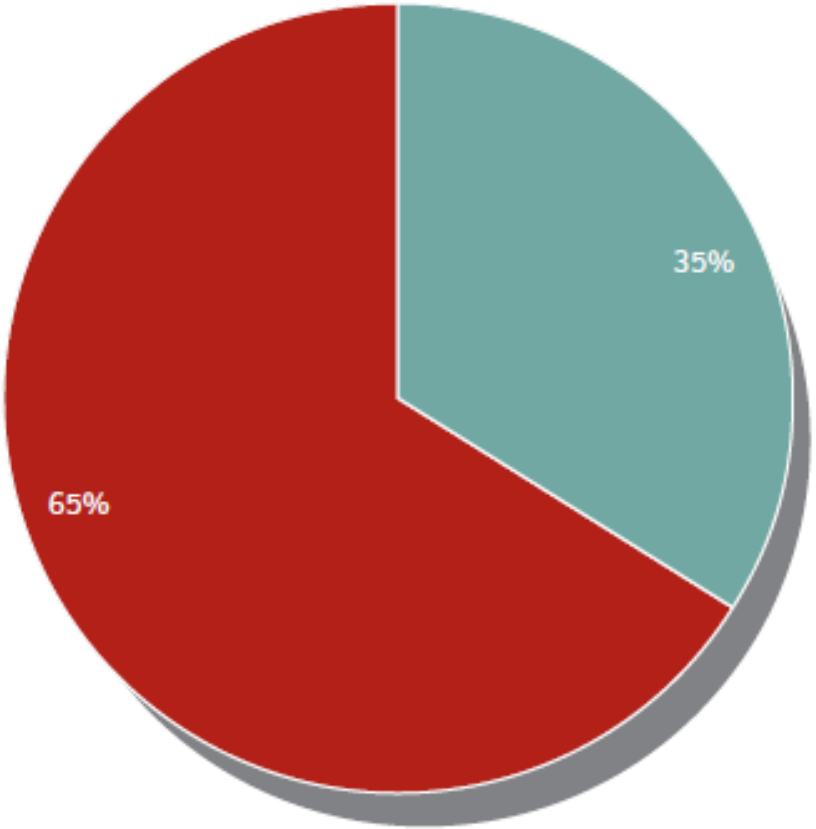
(The Attack Vector)

- Taking a floppy disk to another computer and opening an infected file.
- USB sticks: works best when workstation has 'autorun' enabled.
- Email: Clicking on a link (This goes to a web site which uses an exploit kit to infect your machine) or opening a file received in your email.
- The tinyURL: Often magazines, newspapers or anyone can sign up to have a URL shortened into one that is much smaller for print.

  Ex: http://www.fbi.gov/news/pressrel/press-releases/fbis-top-ten-news-stories-for-the-week-ending-september-9-2011 into **http://tinyurl.com/3q5czrg**

  This is a good way to hide URL's that have exploit kits embedded into the web page.
- Quick Response Codes: Used to send people to a website, often used with a tinyURL to disguise the destination.

Beware the tinyURL



Malicious URLs targeting social networking users over a three-month period in 2010

Source: Symantec Corporation

Quick Response (QR) Codes

- QR Codes have sprung up everywhere in the last couple of years. They are a convenient way to covert a barcode into a website using a camera on a smart phone.
- Used to promote black market pharmaceuticals
- Install a trojan on Andriod Phones.
- Used with the tinyURL very hard to determine if the site is safe or not.

Methods of Attack

(The Attack Vector)

- Browsing to a website. (Typos, False DNS Entries)
- Peer-to-peer file sharing software: The downloaded files can be infected and not to mention might be violating intellectual property laws (copyright.)
- Instant Messaging: Someone can send an infected file or link to a user.
- Social Engineering: Using someone else actions in order to breach security.

  Ex: Help Desk calls you and says, there is an issue with your computer, can I have your user name and password or a popup window says an authentication error occurred and to please enter your User ID and Password.
- Physical Security: Preventing unauthorized access to the workstation or server is very important, since cached passwords can be decrypted.
- Social Networks: Facebook, MySpace, Twitter, etc.

Other Types of Scams

The 419 Scams: The term 419 is a reference to the Nigerian penal code which deals with fraud scams. There are various types of 419 scams:

- Lottery: It usually starts with an email that you have won a lottery, but to get the money you have to pay some sort of upfront fee.
- Inheritance: Similar to the Lottery in method of approach except that you recently have received a large inheritance.
- Need help getting money out of the country
- I want to buy something from you.

All these scams try to accomplish one thing: To separate you the 'Mugu' (Nigerian for fool) from your money.

Other Types of Scams (Continued)

Banner Ad:

In 2009, a hacker used a banner ad on the New York Times website. The group posed as a national advertiser and purchased product advertising for a week. The submitted ad was then replaced with another ad which produced a message claiming to be a virus warning from the user's computer. When a user clicked on the ad, malware would immediately be installed.

- Kravets, D. (2009, September 14). *New York Time Reforms Online Ad Sales after Malware Scam*. Retrieved October 12, 2010, from Wired: http://www.wired.com/threatlevel/2009/09/nyt-revamps-online-ad-sales-after-malware-scam/

Other Types of Scams (Continued)

Search Engine Optimization:

In 2009, fans of the "*Da Vinci Code*," were targeted by an Eastern European group.

"On Tuesday, NBC's Today show kicked off a week-long promotion for Brown's 'Da Vinci Code' sequel by airing the first of a series of clues to the thriller's plot, in the form of a tour of a real-life biological research facility nicknamed the "Death Star" because it houses dead animal specimens. Host Matt Lauer challenged viewers to identify the research site and its location, and thereby acquire vital information about the novel. "Suffice it to say, that this facility is a big part of the book," said Lauer. 'So, if I'm in a place called the Death Star, where am I?'"

-Poulsen, K. (2009, September 9). *'Da Vinci Code' Fans Targeted by Real International Conspiracy*. Retrieved October 12, 2010, from Wired: http://www.wired.com/threatlevel/2009/09/dan-brown/

This group used search engine optimization techniques to enable their code to show up when someone used Google for "Death Star Research."

Protection Methods

Firewalls: A firewall software or a physical device that allows only authorized traffic to pass through.

Anti-Virus/Anti-Spyware: This software works mostly in a few ways:

- *Dictionary*: Uses hashes to determine if the 'signature' of a known threat is present. Polymorphic viruses are designed to defeat this type of defense.
- *Reputation-Based:* Classifies software files into good or bad. Based on large contributions from the install base.
- *Suspicious Behavior Approach (heuristic)*: The software monitors certain processes to see if these have been changed or altered. Often results in many warnings for legitimate changes, and subsequently the user becomes desensitized to its messages.
- *Sandbox*: Software emulates the operating system, runs the suspect code, and monitors the executable to see if it acts like a virus. Extremely processor intensive and not many vendors support it.

Intrusion Detection Systems (IDS): These are often network based systems (hardware and/or software) which look for unusual traffic or access to network resources.

Protection Methods (Continued)

System Updates (Patching): Is the method of installing additional software to enhance security and/or functionality. This method occurs on the Operating System level and for the applications which are installed. A method has been developed to gain access to a system, after the flaw is discovered but before it is patched is called a 'Zero-Day Vulnerability.'

Encryption: Is a method used to disguise data using a mathematical formula.

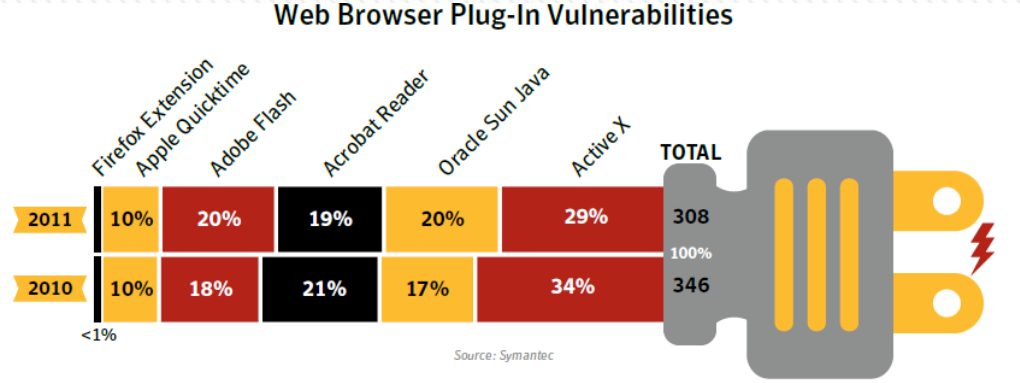
Physical Security: Limiting physical access to the computer or server. Preventing this access will prevent bootable media from being used to circumvent the host operating system. Also, locking your keyboard when anytime you are away from your desk.

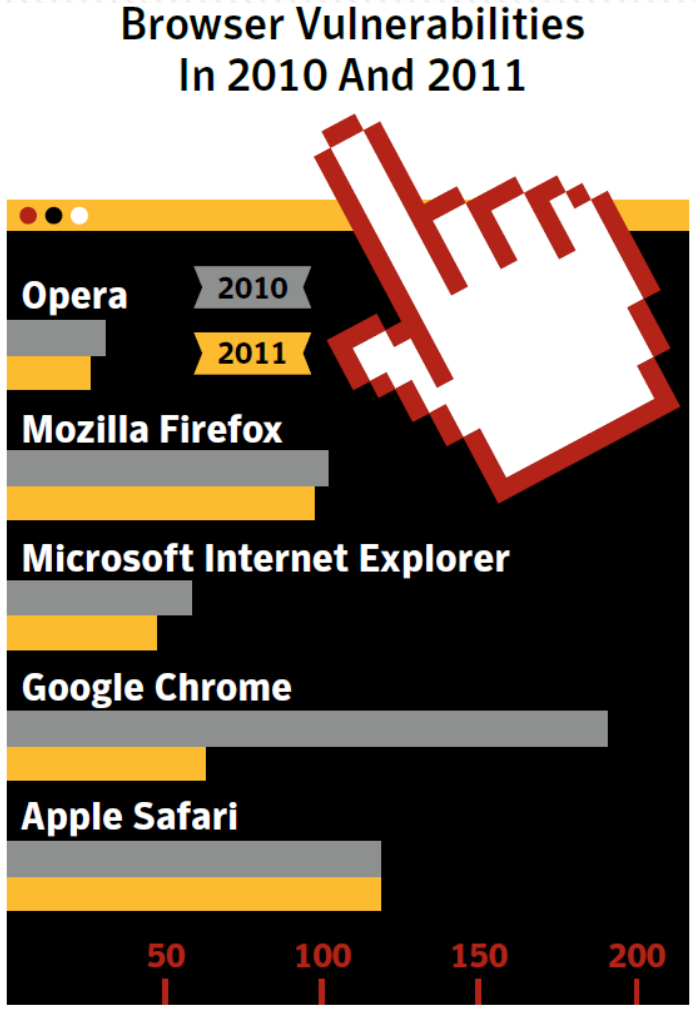
Awareness (knowledge): Being aware of the types of threats, how these threats are deployed, in my opinion, is the best solution. It is one of the most effective solutions because it works with both known and unknown threats to an information system.

Internet Crime Complaint Center Data

"IC3 2010 Annual Report." *Internet Crime Complaint Center.* http://www.ic3.gov/media/annualreport/2011_ic3report.pdf (accessed September, 2012).

Statistics: Web Browser Vulnerabilities





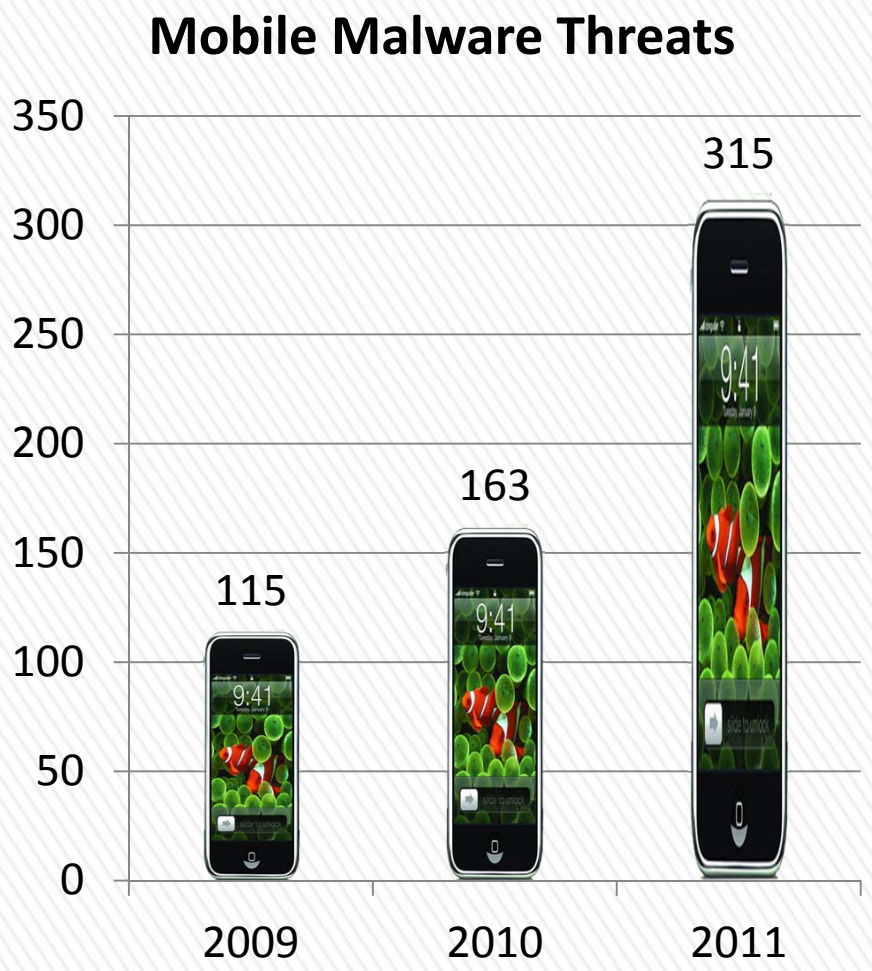
Mobile Phone Threats

2011 saw a significant increase in threats that specifically target ‘smart’ phone users.

Currently, most malicious software for mobile phones consists of a trojans that appear to be legitimate applications.

While most Trojans for ‘smart’ phones simply dialed of texted to premium rate services, Pjapps attempts to create a botnet out of Andriod phones.

Android phones are particularly vulnerable due to the unregulated marketplace.



Mobile Phone Threats (Continued)

iOS vs. Android: Security Overview

The following tables summarize our conclusions about the various strengths and weaknesses of both the iOS and Android mobile platforms.

Table 1

Resisting attack types

Resistance to:	Apple iOS	Google Android
Web-based attacks		
Malware attacks		
Social Engineering attacks		
Resource Abuse/ Service attacks		
Data Loss (Malicious and Unintentional)		
Data Integrity attacks		

Table 2

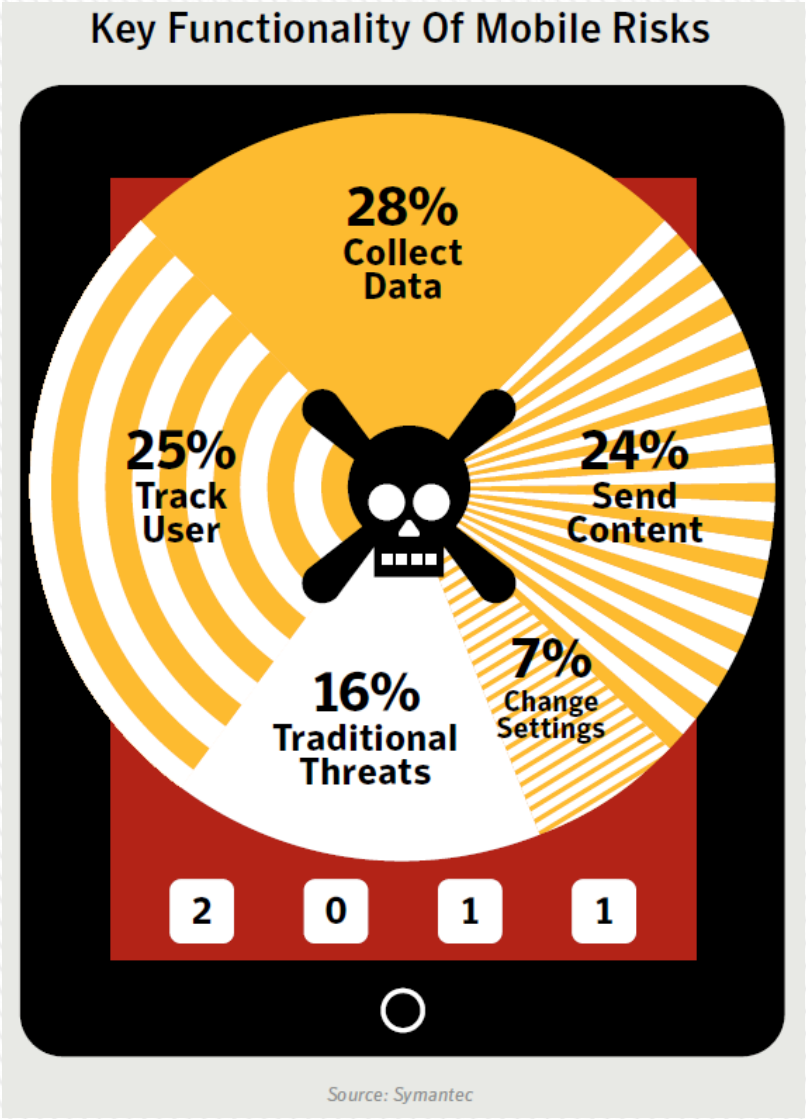
Security feature implementation

Security Pillar	Apple iOS	Google Android
Access Control		
Application Provenance		
Encryption		
Isolation		
Permission-based Access Control		

Legend

- Full Protection
- Good Protection
- Moderate Protection
- Little Protection
- Little or No Protection

Mobile Phone Threats (Continued)



The Year in Numbers

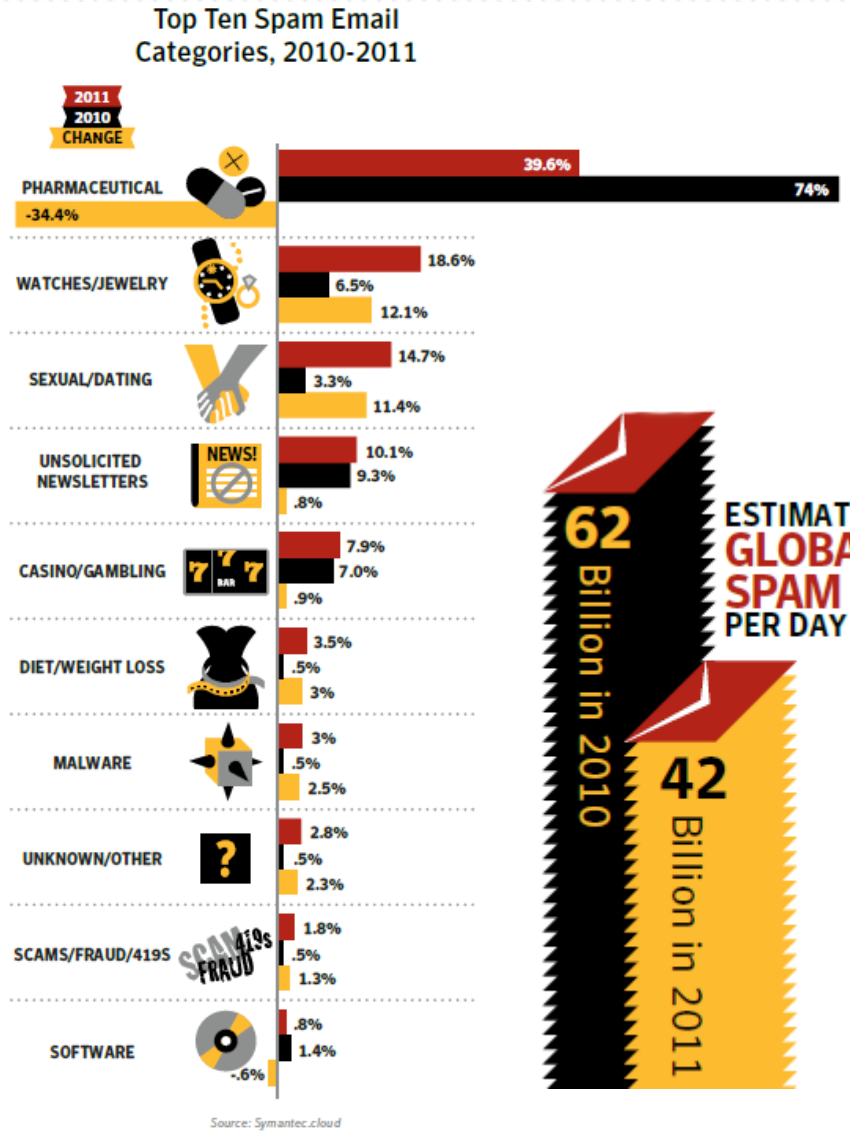
403 MILLION UNIQUE VARIANTS OF **MALWARE** VS. **286 MILLION** IN 2010

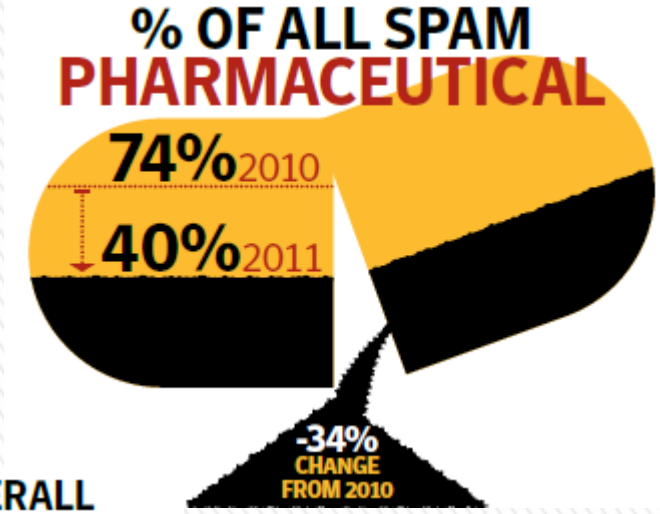
55,294 UNIQUE MALICIOUS WEB DOMAINS VS. **42,926** IN 2010

By Category, The Top-5 Most Infected Websites Are:

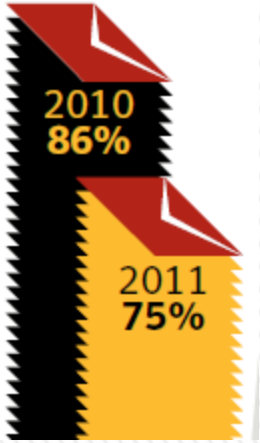
1. Blogs & Web communications
2. Hosting/Personal hosted sites
3. Business/Economy
4. Shopping
5. Education & Reference

The Year in Numbers (continued)

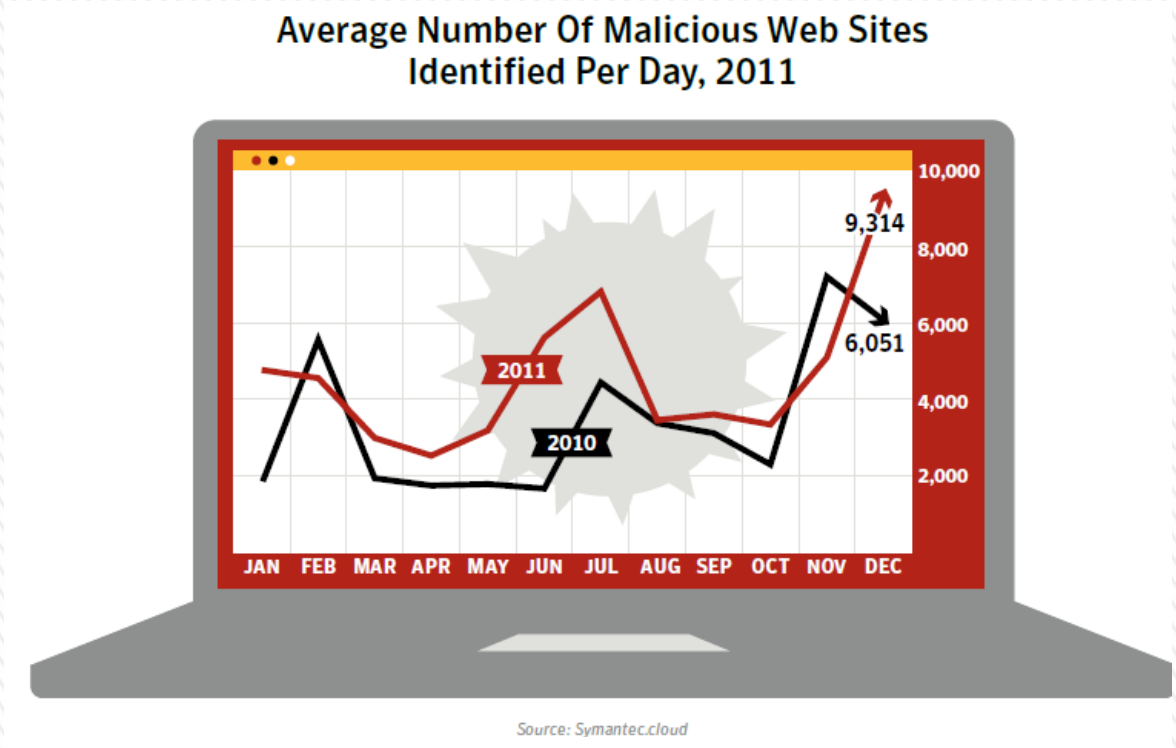




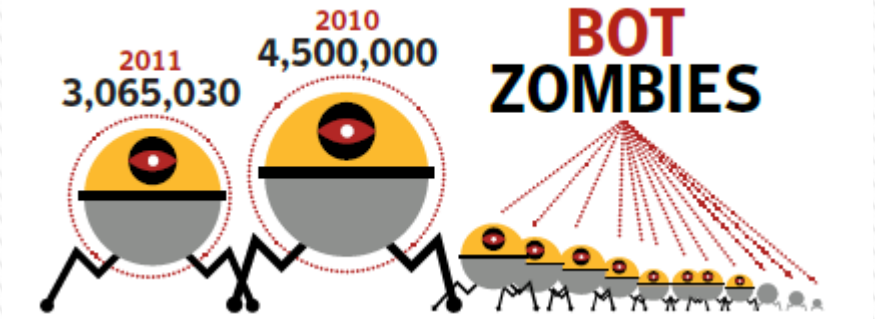
ESTIMATED GLOBAL SPAM PER DAY



The Year in Numbers (continued)



Source: Symantec.cloud



Other Interesting Statistics

- "Cybercriminals have a 10% - 45% chance of getting past your AV with Web Malware (depending on the product)." (NSS Labs 2010)
- "Cybercriminals have between a 25% - 97% chance of compromising your machines using exploits (depending on the product). Over half of the AV products tested stopped less than 50% of the exploit attacks." (NSS Labs 2010)
- "Up to 1/3 of security software contracts change hands every year." (Kirk 2010)
- "Hackers create 57,000 new web pages every week in a bid to infect web users with malicious software." (Skinner 2010)
- "Over 375 keywords or brands are hijacked every week and used in the URLs of these malicious web pages." (Skinner 2010)
- "…25% of new worms are designed to spread via USB devices" (Panda Security 2010)
- 33% of companies were infected with malware by employees using social networking sites. (Panda Security 2010)

Other Interesting Statistics

» Stuxnet: The Stuxnet worm is the first worm of this type specifically designed to attack infrastructure components like power stations and electricity grids. In September, Iran's state news agency announced it new nuclear power plant was infected by Stuxnet.

This is the first time a worm has been discovered that can monitor and reprogram industrial systems. It was specifically written to attack Supervisory Control and Data Acquisition (SCADA) systems used to control and monitor industrial processes. Stuxnet includes the capability to reprogram the programmable logic controllers (PLCs) and hide the changes. (McMillan 2010)

Most experts agree that the Stuxnet worm was most likely the work of some nation, due to its level of technology used in its design, implementation and execution. It used four different zero-day exploits.

Duqu: The next generation of Stuxnet, using 99% of the same software code. It contains a keylogger which stores files with the ~Dox.tmp name. The virus can communicate with command and control servers and can delivered a payload to the infect computer. This virus was initially delivered via a Microsoft Word document and utilized a previously unknown bug to infect the machine. Duqu looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive, the known components are trying to gather information

The Underground Economy

Current figures estimate $1 Trillion dollars is lost in the global economy each year due to cyber related crimes.

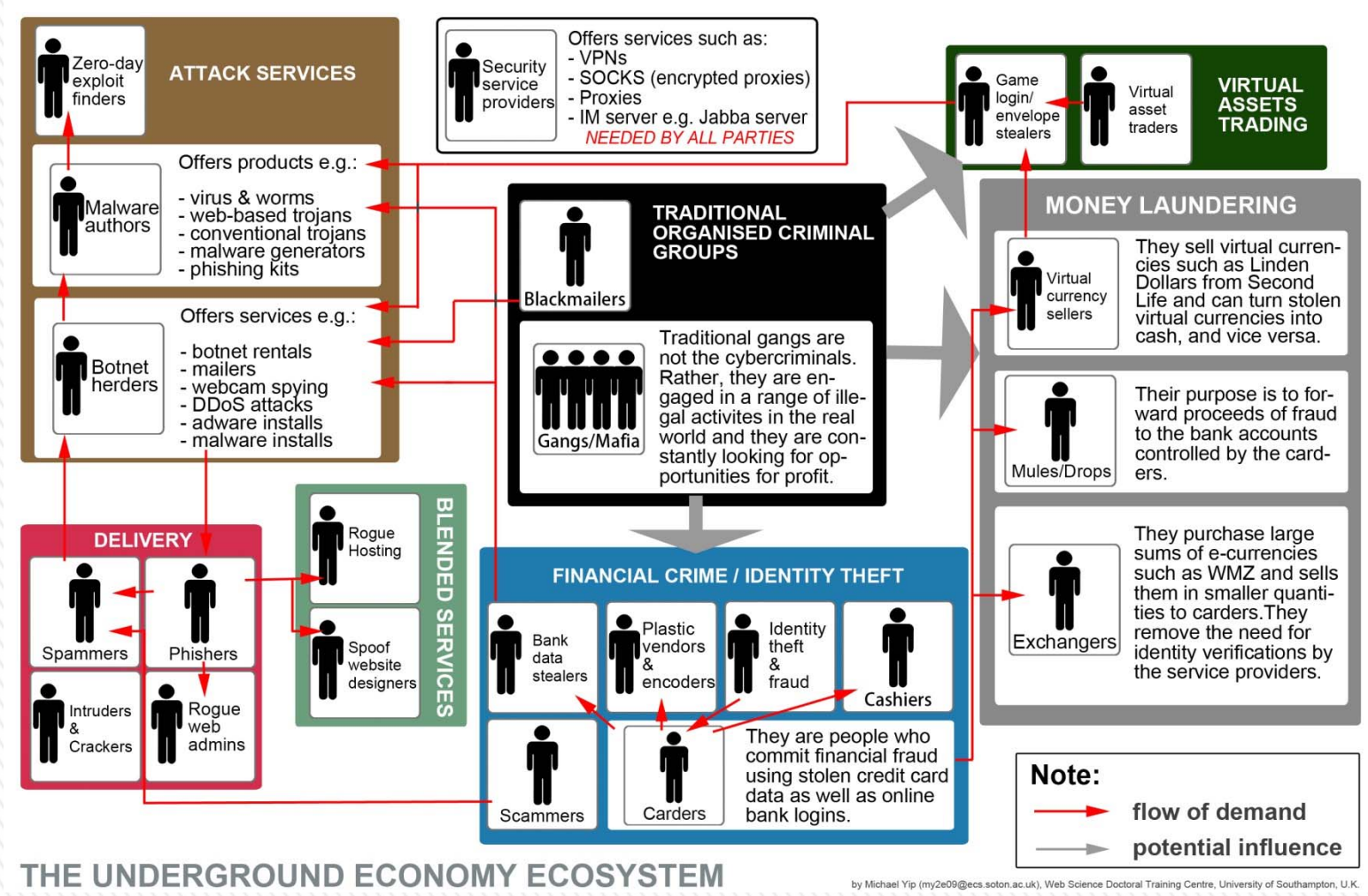
Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec

The Underground Economy

- **Credit card details:** From $2-90
- **Physical Credit Cards:** From $180 + cost of details
- **Card Cloners From** $200-1000
- **Fake ATM Machines:** From $3,500
- **Bank Credentials**: From $80-700 (with guaranteed balance)
- **Money Laundering From:** 10 to 40 percent of the total
- **Design and publishing of fake online stores:** According to the project (not specified)
- **Purchase and Forwarding of Products:** From $30-300 (depending on the project)
- **Spam Rental:** From $15
- **SMTP Rental:** From $20 or $40 for three months

The Ecosystem



THE UNDERGROUND ECONOMY ECOSYSTEM

by Michael Yip (my2e09@ecs.soton.ac.uk), Web Science Doctoral Training Centre, University of Southampton, U.K.

How Serious Is This?

» The US Military has established the US Cyber Command to combat threats to our nation.

> *"On June23, 2009, the Secretary of Defense directed the Commander of the US Strategic Command to establish USCYBERCOM."* (Cyber Command Fact Sheet, 2010)

> *"…the Pentagon's computer systems 'are probed 250,000 times an hour, up to six million per day' and that among those attempting to break in were 'more than 140 foreign spy organizations trying to infiltrate US networks.'"* (Glenny, 2010)

» Air Force Basic Training now includes a four hour course in basic cyber security.

» Keyloggers has been found in Creech Air Force Base's classified and unclassified systems information systems.

» Air Force Unmanned Aerial Vehicles were infected by USB sticks used to upload maps.

» Reports show that ~ 70% of Armed Forces data breaches are caused by unauthorized use of USB sticks.

Who's been hacked?

- **Yahoo (July 2012):** 450,000 usernames and passwords. Stored passwords in plain text inside database.
- **LinkedIn (June 2012):** Six Million passwords stolen and posted on Russian web site.
- **Ministry of Defense (UK, May 2012):** Top Secret systems compromised.
- **Environmental Protection Agency (March 2012):** 8,000 peoples' Social Security Numbers, bank account information, and home addresses. User open email attachment.
- **Global Payments (March 2012):** Company which processes debit and credit card transactions lost 56,000 account numbers to hackers.
- **Department of Defense (February 2012):** F-35 development program was compromised by Chinese hackers.
- **Department of Justice (January 2012):** The group Anonymous took down DOJ websites including the FBI website, protesting the FBI shutting down megaupload.com.

What should I do?

- Update Antivirus and Antispyware software (daily).
- Update operating system on a regularly.
- Update your applications when available.
- Backup your files often.
- Use a complex password (upper case, lower case, symbol, and numbers) that is at least 8 characters long and change it frequently.
- **Do not** share your password.
- **Do not** open any files or attachments from people you do not know!
- **Do not** open files or attachments from people you do know, if you are not expecting it or do not know what it is.
- **If it is too good to be true, it most likely is!** So do not even bother responding. If you do respond, you will not only waste your time, but you will also confirm your email address as a good one. The following are examples:
  - **YOU DID NOT JUST WIN THE LOTTERY!!** Do not send money or anything else to these people. This is true no matter what they say. (Watch me be wrong with this…)
  - Someone you never heard of is not willing to split a fortune with you if you just send them a fee…

What should I do?

(do these slides ever stop…)

- Be wary of free software on the Internet.
- Only download software from trusted sources. (CNET, Microsoft, developer, etc.)
- **Do not** click on a Yes, No, OK or Cancel button in a popup. Click on the 'X' (close) button in the top right if at all possible. A button can be programmed to do anything, but it is much harder to override the windows form control (the X).
- **Turn off Autorun:** Turn off the ability to autorun software on removable media, such as a USB stick, when it is inserted.
- **Do not** use Pirated software.
- **Lock** your workstation or **logoff** when you leave your desk.
- Be careful who or what you give your personal information too. Often when signing up for something on the web, these sites ask for way more information than it should have.
- Beware of the tinyURL…
- **And finally… Be Aware and Be Cautious.** *(Scan the horizon for the next threat).*

Tools and Information

- National Cyber Security Alliance (http://StaySafeOnline.org): Has many links and references to cyber security lessons and tips for the classroom.
- OnGuard Online (http://www.onguardonline.gov/): Provides tips from the federal government and the technology industry to help you be on guard against internet fraud, secure your computer, and protect your personal information.
- NetSmartz Workshop (http://www.netsmartz.org/index.aspx): The website from the National Center for Missing and Exploited Children has resources for Educators on cyber safety.
- CyberSmart (http://www.cybersmart.org): Information on safety, security, cyber bullying and cyber citizenship.
- Threat Expert (http://www.threatexpert.com/default.aspx): Site used to submit virus samples to with very detailed reporting. I used this site to determine how a new stain infected a machine, and how to create a specialized cleaner to eliminate it.
- McAfee (http://vil.mcafeesecurity.com/vil/submit-sample.aspx): Allows submission of suspected code for analysis.

Works Cited

- Blunden, Reverend Bill. *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System.* Plano, Tx.: Wordware Publishing, Inc., 2009.
- "Cyber Command Fact Sheet." *Department of Defense.* October 13, 2010. http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYBERCOM%20Fact%20Sheet%20to%20replace%20online%20version%20on%20OCT%2013.pdf (accessed October 17, 2010).
- Glenny, Misha. "Who controls the internet?" *Financial Times.* October 8, 2010. http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html (accessed October 14, 2010).
- "IC3 2011 Annual Report." *Internet Crime Complaint Center.* http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf (accessed September 26, 2011).
- Joseph, Mike. *BMT begins cyber training.* October 14, 2010. http://www.lackland.af.mil/news/story.asp?id=123226441 (accessed October 17, 2010).
- Kirk, Jeremy. "Tesing Reveals Security Software Often Misses New Malware." *ComputerWorld.* June 20, 2010. http://www.computerworld.com/s/article/9178338/Testing_reveals_security_software_often_misses_new_malware (accessed October 15, 2010).
- Knight, Will. "A Year Ago: Cypherpunks Publish Proof of Tempest." *ZDNet UK.* October 26, 2000. http://www.zdnet.co.uk/news/security-management/2000/10/26/a-year-ago-cypherpunks-publish-proof-of-tempest-2082190/ (accessed October 13, 2010).

Works Cited (Continued)

- Kravets, David. *New York Time Reforms Online Ad Sales after Malware Scam.* September 14, 2009. http://www.wired.com/threatlevel/2009/09/nyt-revamps-online-ad-sales-after-malware-scam/ (accessed October 12, 2010).
- McMillan, Robert. "Siemens: Stuxnet worm hit industrial systems." *ComputerWorld.* September 14, 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142 (accessed October 12, 2010).
- NSS Labs. *Consumer Anti-Malware Products Group Test Report.* Research, Carlsbad: NSS Labs, 2010.
- Panda Security. "Quarterly Report PandaLabs (July-September 2010)." *Panda Security.* October 2010. http://prensa.pandasecurity.com/wp-content/uploads/2010/09/Quarterly-Report-PandaLabs-3-Q-2010.pdf (accessed October 17, 2010).
- Panda Security. "Quarterly Report PandaLabs (July-September 2010)." *Panda Security.* October 2010. http://press.pandasecurity.com/wp-content/uploads/2012/01/Annual-Report-PandaLabs-2011.pdf (accessed October 1, 2012).
- Poulsen, Kevin. *'Da Vinci Code' Fans Targeted by Real International Conspiracy.* September 9, 2009. http://www.wired.com/threatlevel/2009/09/dan-brown/ (accessed October 12, 2010).
- Shachtman, Noah. *'Computer Virus Hits U.S. Drone Fleet.' by WiredOctober 3*, 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/ (accessed October 16, 2011).
- Skinner, Carrie-Ann. "Hackes Create 57,000 Malicious Pages Each Week." *PCWorld.* September 11, 2010. http://www.pcworld.com/article/205310/hackers_create_57000_malicious_pages_each_week.html (accessed October 16, 2010).
- Symantec. "Symantec Internet Security Threat Report Trends for 2011, Volume XVII." *Symantec.* April 2012. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (accessed October 2, 2012).
- Yip, Michael. *'The Underground Economy Ecosystem'.* August 31, 2011. http://www.michaelyip.me.uk/blog/2011/08/the-underground-economy-ecosystem/ (accessed October 12, 2010).

Questions?

Copies of this presentation will be at:
http://www.digimechs.com/