UTICA COLLEGE
ONLINE DEGREE PROGRAMS

Cyber Threat Overview

Dr. Len Popyack
Utica College
Nov 2011

Cybersecurity- Intelligence and Forensics

Overview

- Spam: Top Threats
- Malware: Top Threats
- Botnets
- Malicious Websites
- Bitcoins

Malcode Lifecycle

- Access – getting initial execution ability
  - Droppers, exploits, USB drive, CD, etc
- Hiding & Sequencing
- Communication, propagation, establishment
- Self-protection
- Operation

Spam: Top Threats

- Spam: unsolicited email
- Used to gain access, fraud, propagation of malware, phishing schemes, etc
- Turbulent spam activity throughout 2010 & 2011
  - average spam levels 72.9%-April 2011 89.1% in 2010
  - 2010: High 92.2% Aug
  - compromised computers issuing 77% of all Spam
  - 339,600 different malware strains identified in emails
  - 1 in 235.8 emails contain malware
- Current level is 74.2% Oct 2011

Web Malware & spyware

2010
New sites with malware
3,066
/day

Oct 2011: **3,325 / day** -- New Malicious Web sites

data from Symantec Intellig□ence reports

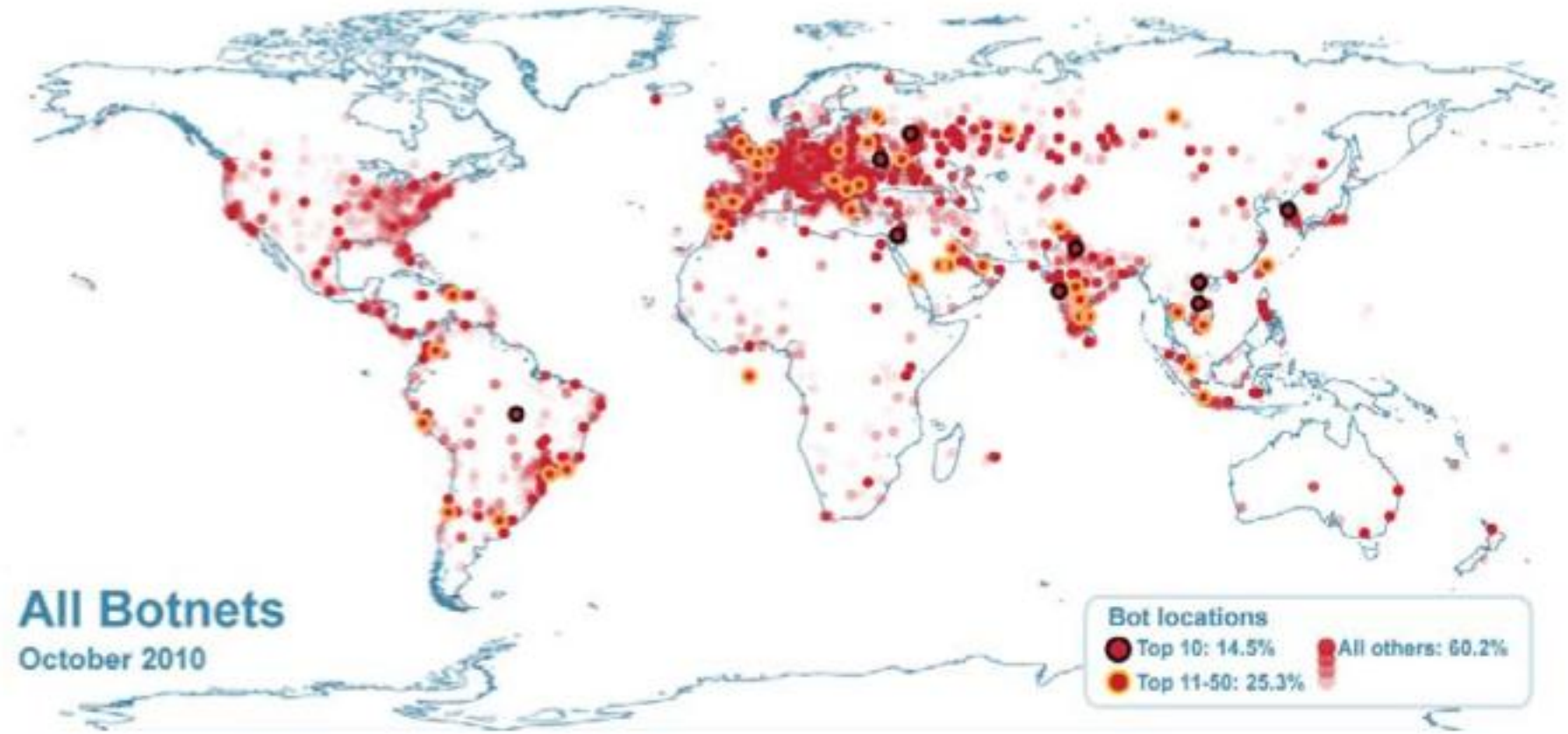
Botnets

- An established collection of malware which can be collectively controlled to perform tasks
- Generally on a compromised computer, well hidden with broadband internet access
- Botnets are the army's of civilian cyber war
- Owners rent time & resources of the botnet to other bad guys

Top Botnets

- Rustock 47.5% (1.1M-1.7M bots)
- Grum 8.5% (310k-470k)
- Cutwail 6.3% (560k-840k)
- Maazben 5.2% (510k-770k)
- Mega-D 2.3% (80-120k)
- …. On and on..

Global bot locations



from annual Symantec Intellig□ence report

Botnet Command & Control

- Traditionally has been IRC channels
- Now changing
  - Using HTTP Channels
  - Covert Channels
- New Technology
  - Fast Flux based domain name services
    - DNS technique used to conceal the addresses of websites used to host malware
  - Using Social Networking services and APIs
  - Web 2.0 consolidate multiple data streams from diverse unrelated sources
- Average size of spam <5Kb

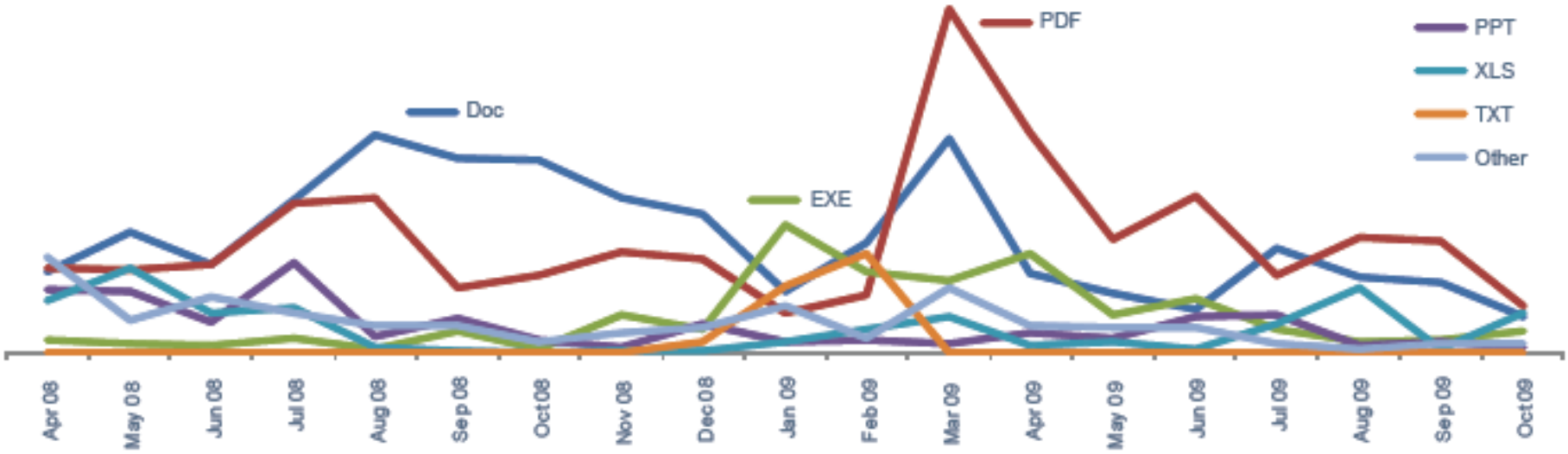
Malware Top Threats

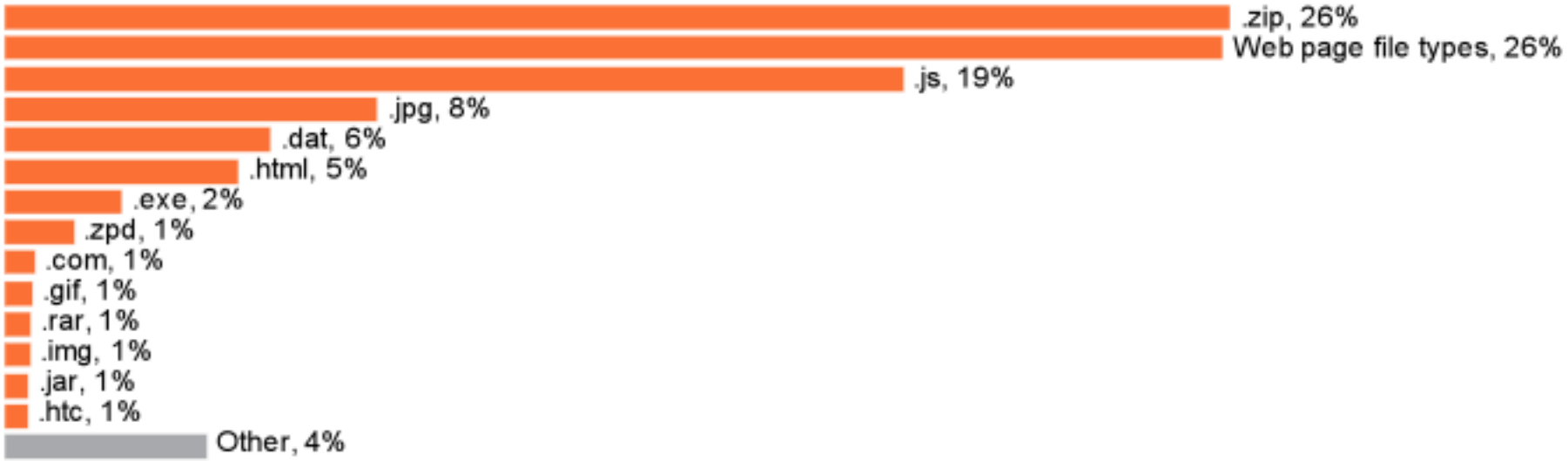
- email-borne malware, the average virus level for 2009 was 1 in 286.4 emails (Aug 2011- 1 in 203.3) Current 1 in 235.8
- 23% increase strains in 2009 compared with 2008
- 73.1+ million malware infected emails were blocked of over 3,441 different malware strains
- This was an average of more than 5,800 malicious emails per strain
- Master Boot Record infections are back in

Targeted Attacks

- ultimate aim of a targeted attack is to gain access to sensitive data or internal systems by targeting specific individuals or companies
- Usually stealth deployment of an executable
- frequently they are hidden within very legitimate looking documents such as .PDF, .DOC, .XLS, .PPT

Types of Apps & Exploits





from annual Symantec Intellig□ence report

Who is Targeted?

- Government/Public Sector 34.7%
- Finance 10.6%
- Professional Services 7.7%
- Education 7.1%
- Manufacturing 7.0%

% of Global Targeted Trojan Attacks

Malicious Websites

- Over 30,000 tracked sites
- New Technology: server-side polymorphism
  - the same family of malware code may be packaged differently into new strains, automatically and dynamically, each time it is accessed
  - The polymorphic engines do not reside within the malware itself, but remotely
    - cannot be analyzed readily for creating signatures.

Bitcoins

- A recent form of Internet ‘money’
- A paper by an unverified self-published author, Satoshi Nakamoto, 2008
- Bit-torrent inspired peer-to-peer currency
- Cryptographically generated, or ‘mined’
- Currently 7 Million bitcoins. Maximum 21 Million. Can be used fractionally

Bitcoin P2P Digital Currency

Bitcoin is an experimental new digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out **collectively by the network.** Bitcoin is also the name of the open source software which enables the use of this currency.

The **software** is a community-driven open source project, released under the **MIT license.**

Learn how to use Bitcoin »

Learn more about Bitcoin »

Download

Latest version: 0.4.0

- Windows (zip) ~8MB
- Windows (exe) ~4MB
- Linux (tgz, 32/64-bit) ~12MB
- Mac OS X ~6MB

or get the source code (GitHub)

Resources

- We Use Coins. Start here!
- Bitcoin Wiki
  - FAQ
  - Sites That Accept Bitcoin
  - Merchant Howto
- Bitcoin Charts / Markets

Developers

- Satoshi Nakamoto
- Gavin Andresen - gavinandresen@gmail.com (PGP)
- Pieter Wuille
- Nils Schneider - nils.schneider@gmail.com (PGP)
- Jeff Garzik - jgarzik@exmulti.com (PGP)
- Wladimir J. van der Laan - laanwj@gmail.com (PGP)

Press mailing list for presentation and interview requests:
bitcoin-press@lists.sourceforge.net

Community

- Bitcoin Stackexchange (Q&A)
- Visit the unofficial Bitcoin Forums
- Join the project's lively IRC channels on the FreeNode network or use the FreeNode Web IRC.
  - **#bitcoin** (General Bitcoin-related)
  - **#bitcoin-dev** (Development and technical)
  - **#bitcoin-otc-foyer** (Over The Counter exchange)
  - **#bitcoin-market** (Live quotes from markets)
  - **#bitcoin-mining** (GPU mining related)
- Twitter Search
- Facebook Page

Bitcoin version 0.4.0 released

23 September 2011

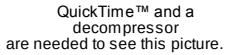
Full announcement (including signatures)

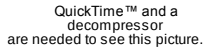
Bitcoin version 0.4.0 is now available for download at: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.4.0/

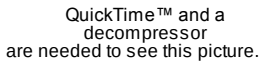
The main feature in this release is wallet private key encryption; you can set a passphrase that must

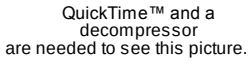
European Conference

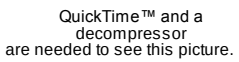
The Bitcoin European Conference (Nov 25—27) will bring together diverse people from across the spectrum to discuss the state of bitcoin and plot future goals. This 3-day conference covers the cutting-edge of developments and innovation through sessions that encourage interaction and discussion between


QuickTime™ and a
decompressor
are needed to see this picture.

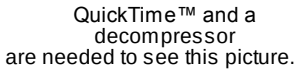

QuickTime™ and a
decompressor
are needed to see this picture.

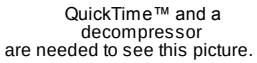

QuickTime™ and a
decompressor
are needed to see this picture.


QuickTime™ and a
decompressor
are needed to see this picture.

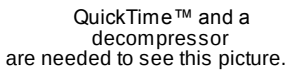


I2P is a self-managed distributed Darknet. A user does not have to advertise their site if they don’t want to.


QuickTime™ and a
decompressor
are needed to see this picture.


QuickTime™ and a
decompressor
are needed to see this picture.

100,000 size botnet x $150 each=$15 M USD/month



Credits

- MessageLabs Intelligence (a Symantec company)
- Microsoft
- Rootkit.com
- Verizon Business reports
- Bitcoin websites
- I2P sites