NUIT Tech Talk

Beating Back the Tide (of Security Exploits)

***

Information & Systems Security/Compliance

***

May 3, 2011
“Thank You” to RSA
The Security Division of EMC Corp.

Etay Maor – Head of Fraud Action Knowledge Delivery

Rachael Stockton – Senior Manager, Product Marketing

Dave Kovarik, Director
Information & Systems Security/Compliance
Overview

• What’s happening
  • Significant increase in activity, all OS, all devices
  • Increased sophistication

• What we’re doing
  • Scanning
  • Assessments
  • Communications
  • Prevention

• What You Can Do
  • 100% Aware
  • 100% of the Time
Communication Sophistication

10's
- Mobile phones, tablets, etc.
- Access from/to everywhere

90's
- Multi-use machines
- Work & personal use
- Remote access

80's

70's
- Dedicated machine
- Specific transactions and locations

60's
Advanced Persistent Threats (APT)

Operation Aurora
- Highly Targeted, Highly Coordinated
- Targeted Unpatched Vulnerability
- Able to Bypass Most Common Security Controls

Malware Infection
- Targeted or Widespread
- Botnet Application, Bulletproof Hosting
- SaaS Capable

Spear Phishing
- Targeted, Coordination Varies
- Relatively low-tech
- Buy mailing list online
Growth In Mobile Platforms

- Mobile applications have more than tripled over the past year
- App downloads are expected to increase sevenfold within the next five years
- Device and mobile delivery platform diversity will continue to expand
Targeting Mobile Platforms

SMS Bomber Application:
- SMS-Short Message Service
- Automated spamming
- Leverage multiple source e-mail accounts

SaaS:
- $7/100 SMS
- $20/500 SMS
- $35/1000 SMS
Mobile Specific Malware

Facebook Called Biggest Threat For Mobile Malware

Google Zaps Rogue Android Apps

By Giles Turnbull on March 2, 2011

News

Fortify warns users of iPhone malware

19 April 2010

With Apple finally announcing what will and won't be seen in v4.0 of the iPhone operating system, Fortify Software has warned users to watch out for its multitasking aspect as it may hide malware running in the background.

JAILBREAKING: Contributing Factor
Customization
Continued popularity and now with variations…

- **Phishing**: E-mail, Instant Messaging
- **SMiShing**: Text message and malware download
- **Vishing**: Voicemail, use of synthesized messages, VoIP features, Caller-ID spoofing

*Chart Data: RSA 2010 Global Online Consumer Security Survey*
“Stand Alone Attack”
• No need for hosting, domains or page design
• Simple yet successful
• Consumer education still best prevention
Multiple and New Targets and Schemes

- Simultaneously target consumers of multiple products/services
- Using social engineering schemes (tax refund, satisfaction surveys, etc.)
- Collecting financial information but not targeting financial institutions
Competition parallels legitimate business

- Free Market, Responsive pricing
- Better Features = Product Sales
- Full SLAs
- No shortage of product

Customer hijacking
- SpyEye cleans ZeuS before installation

Cooperation focuses efforts

- Attention paid to product enhancement
- Increased functionality
- Broader fraud community input
- Credit card grabbing add-on application
- Windows Remote Desktop application Backconnect
Backconnect

- Bad Guy inserts malware into video
- Bad Guy executes netcat command
- Bad Guy sends out video
- Good Guy executes video
- Bad Guy owns Good Guy

[Video]
Trojan SaaS

Uhoax

Join Date: Nov 2010
Posts: 5
Rep Power: 0

Complete SpyEye Service

Hello members of MyMarket,
Today I present you all my service of SpyEye Botnet Installation.
What will you receive from the service?

- BULLETPROOF hosting, server located in Lithuania for 3 months.
- BULLETPROOF ABUSE domain, registered true 3rd party registrar for 1 year.
- 1000 RANDOM MIX bots (can give specific country also, if available in stock)
- LATEST AJAX POP-UP webinjeds for all major countries.
- UNLIMITED number of bin building to same domain. Domain change $100. If the domain gets locked (99% it will not) I will build bin on your new domain for free of cost.
- UPDATED .htaccess configuration to block SpyEye tracker.
- Noob friendly support. No matter what problem you face, I am here to help you out.

Bin’s are created from SpyEye version 1.2.99.29 (latest)

Price of the service is $800.
Payment gateway is LibertyReserve only.
Escrow is accepted and buyer pays the fees.

Contact me in PM if you are interested.

Last edited by Uhoax; 01-05-2011 at 06:02 AM.
Zeus V. 2.0.8.9 - Install Service

Zeus 2.0.8.9
I have the pleasure to sell Zeus Botnet version 2.0.8.9.

Description of my services:

Code:
- Installation service on your host.
  - Or on my bulletproof hosting (1 month free then 105 $ per month).
  - FUD support. (1 crypter FUD after the purchase).
  - Windows 7 compatible.
  - VNC + Webinject ours or yours.

Warning:

Code:
1. I does not sell the builder. Just the installation total as well as final bot (FUD).
2. Liberty Reserve payment

Price:

Code:
650 $ Full installation + Stable support.

Contact:

Code:
601100585
More: Malware in 2010

- During 2010, more than 15 new Trojans released
- Each belonging to a different criminal gang
- Developed for internal use or for commercial purposes

Nimkey, Mimicker, Lamp, Bancos, Qakbot, Silon, Gozi, Syscron
The Shift in Malware Threats

From amateur virus writers to organized money making professionals!
The Faces Have Changed

Chen-Ing Hau, 24
(author of CIH virus)

Jeffrey Lee Parson, 18
(author of Blaster.B virus)

Joseph McElroy, 16
(Hacked into Nuclear US Lab)

Script Kiddies
The Faces Have Changed

Jeremy Jaynes
Millionaire spammer

Jay Echouafni
Attacker

Andrew Schwarmkoff
Russian phishing mob

Professionals
HTML Injection
What We’re Doing

- Automated scanning using NESSUS
  - Ongoing and automatic
- On-demand assessments using WebInspect
  - Collaborative process
  - Network, server and applications
- QualysGuard
  - SaaS – scheduled and on-demand
  - Web application scanning
  - Historical reporting
- Communications & Education
Be 100% Aware 100% of the Time

- Enable a firewall on your computer
- Get the latest computer updates for all your installed software
- Keep OS and applications current
- Use up-to-date antivirus software – keep it current
- Limit access to your computer (work vs. personal)
Be 100% Aware 100% of the Time

- Use caution when opening attachments and accepting files
- Use caution when clicking on links to web pages
- Don’t download software you haven’t paid for
- Protect yourself against social engineering attacks
- Use strong password
Probably NOT a good idea

Instead... Get Professional Help
847-491-HELP
Final Thoughts

“You know, you can do this just as easily online.”
REFERENCES

NUIT Support Center 847-491-HELP (4357)
•  www.it.northwestern.edu/supportcenter/

Information Security Flyers
•  www.it.northwestern.edu/security/flyer.html

Phishing E-mail
•  www.it.northwestern.edu/security/phishing.html

Security News Podcasts
•  www.it.northwestern.edu/security/podcast.html

Security Statistics
•  www.it.northwestern.edu/about/stats/sec.html

Secure IT @ NU
•  www.it.northwestern.edu/security/