Trends in the Threat Landscape:
Joshua Rosenthal at the eCampus Security 2012 Conference

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

The annual Securing the eCampus conferences< http://www.ists.dartmouth.edu/events/ecampus/ > are a valuable and enjoyable opportunity for security experts interested in security at educational institutions. Organized by staff of the Institute for Security, Technology, and Society (ISTS)< http://www.ists.dartmouth.edu/about/ >, these conferences have been hosted at Dartmouth College in Hanover< http://www.hanoverchamber.org/ >, New Hampshire< http://www.visitnh.gov/ > since 2007.

This year Joshua Rosenthol< http://www.ists.dartmouth.edu/events/ecampus/bios/rosenthol.html >,CISSP of Websense Labs< http://securitylabs.websense.com/ > presented an excellent overview< http://www.ists.dartmouth.edu/docs/ecampus/2012/2012ecampus_rosenthol.pdf > of the changing Internet threat landscape.

Websense Labs reported on current Adobe Reader vulnerabilities. Key exploits include

- Blackhole 1.1.0 < http://malwareint.blogspot.com/2011/08/black-hole-exploits-kit-110-inside.html
- Phoenix 2.0, 2.3-2.5, 2.7< http://malwareint.blogspot.com/2011/10/inside-phoenix-exploits-kit-28-mini.html >
- Crimepack 2.2.1, 2.2.8, 3.0.0< http://www.inreverse.net/?p=1401 >
- Bleeding Life 2.0< http://krebsonsecurity.com/2011/01/exploit-packs-run-on-java-juice/#more-6876 >
- Impassioned Framework 1.0< http://krebsonsecurity.com/2010/07/pirate-bay-hack-exposes-user-booty/#more-3337 >
- Katrin Exploit Pack< http://cyb3rsleuth.blogspot.com/2011/05/katrin-exploit-pack.html >.

One startling statistic is that if users apply patches immediately when they are released, they nonetheless suffer 104 days of exposure! The speaker quoted an IDC *Threat Intelligence Update* from 2012-02-14< http://www.idc.com/getdoc.jsp?containerId=prUS23290912 > that found that "Signature based tools (anti-virus, firewalls, and intrusion prevention) are only effective against 30-50% of current security threats. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly."

Websense Labs characterize the Web threat lifecycle into the following stages:

- Lure: social-engineering tricks such as YouTube scams, gift offers, natural-disaster relief appeals, targeted spam, and e-mail about specific events and alerts, fake surveys, blog postings (Oh no! Say it ain't so!);
- Redirect: concealing the actual destination of links;
- Exploit Kit: malicious programming to exploit holes in Adobe products, Java, browsers and even TrueType fonts;

- Dropper File: fake antivirus programs, malicious apps, browser plugins;
- Call-Home and Data Theft: data transfer applications that copy and transmit confidential data, including password files.

Websense Labs' ThreatSeeker Network< http://www.websense.com/content/ThreatSeeker.aspx > relies on "the world's first Inernet HoneyGrid." This system "…is a network of technology and human intelligence that creates an adaptive feedback network that uses more than 50 million real-time data collecting systems to parse one billion pieces of content daily.

The presentation closed with the following ranked predictions for 2012:

1. Social Media accounts and targeted attacks
2. Mobile attacks
3. SSL traffic creating blind spot
4. Containment is new prevention
5. London Olympics, US Presidential Election.

I'll finish with my own recommendations for everyone:

- Be on your guard: do not open e-mail from strangers casually.
- Have your antimalware and antiphishing tools online and up to date at all times.
- Convert HTML e-mail to ASCII automatically.
- Verify that the address of a link matches the label for the link exactly.
- Be suspicious of links in top-level domains you don't normally interact with; e.g., if you never have e-mail from Russia or business in France, don't click on a link to URL in .RU or in .FR without careful consideration.
- Block e-mail encoded in languages you do not speak; e.g., if you don't speak Chinese, reject e-mail from .CN.

The full *Websense 2012 Threat Report*< http://www.websense.com/content/websense-2012-threat-report-download.aspx > is available free with simple registration.

My thanks to Joshua Rosenthol for his informative lecture and to ISTS for inviting him to speak.

* * *

[Disclaimer: M. E. Kabay has no relationship whatever with Websense (except for appreciating their research and publications) or with ISTS (except for enjoying their conferences, their publications and their wonderful staff).]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *