

Contact: Alan Paller, paller@sans.org, 301-951-0102x108

**SANS INSTITUTE
PRESS UPDATE**

**2006 Annual Update on SANS Top 20 Internet Security Attack Targets
Shows Marked Increase in Targeted Attacks and
A Human Error Joins the Top 20**

WASHINGTON, DC. –The SANS Institute today announced the 2006 update to the Top 20 Internet Security Vulnerabilities, this year called the Top 20 Attack Targets. This announcement was made in London, in conjunction with the National Infrastructure Security Coordination Centre of the United Kingdom.

The update enables cyber security professionals to tune their defensive systems to reflect the most important new vulnerabilities that attackers are actively exploiting to take over computers and sensitive or valuable information. **This announcement comes in the midst of an explosion in cyber crime, driven in part by a surge in the number of online criminals in Asian countries along with continuing growth in attacks from Eastern European countries. The surge is so great that several banks have reported 400 to 500 percent increases in losses to cyber fraud from 2005 to 2006.** The SANS 2006 Top 20 list sharply illuminates the specific vulnerabilities that these criminals are exploiting to steal or extort money. The list further highlights vulnerabilities that nation-states are using to penetrate British, US, and Canadian military and military contractor sites and other government sites to steal sensitive information and take control of the computers.

Six major trends in attack patterns can be seen in the update:

1. Surge in zero-day vulnerabilities and attacks that go beyond Internet Explorer to target other Microsoft software.
2. Rapid growth in attacks exploiting vulnerabilities in ubiquitous Microsoft Office products such as PowerPoint and Excel.
3. Continuing growth in targeted attacks.
4. Evidence of much greater penetration of military and government contractor sites using spear-phishing attacks; likely heralding a spread to target other types of organizations.
5. VOIP (Voice over Internet Protocol) attacks used now to make money by reselling minutes and potentially for injection of misleading messages and even for creating massive outages in the old phone network.
6. Massive and still increasing exploits of vulnerabilities in web applications.

The release of this list of major new attack patterns does not mean that attackers have stopped using patterns we announced in earlier updates. For example Apple computers are continuing to be targeted – and a new exploit for Apple's wireless capability is just being released. In reality, few attack patterns are ever discarded. The attacks are

automated and continue to be used, but many organizations have established defensive strategies to minimize the risk from the older attack patterns.

Several of the world's top cyber security experts joined forces to ensure the latest and best available information is embodied in the SANS consensus update:

- Rohit Dhamankar, Editor of the SANS Top 20, and Senior Manager of Security Research at TippingPoint, a division of 3Com
- Dr. Johannes Ullrich, Chief Technology Officer, SANS Internet Storm Center
- Gerhard Eschelbeck, Chief Technology Officer, Webroot
- Amol Sarwate, Manager, Vulnerability Management Lab, Qualys
- Ed Skoudis, SANS "Hacking Exploits" Course Director and Senior Security Analyst, Intelguardians
- Marc Sachs, Director, SANS Internet Storm Center, and SRI International
- Alan Paller, Director of Research, the SANS Institute