

**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

## Expert Analysis

### VoIP

Last year we saw many remote code execution vulnerabilities in Asterisk, a popular VoIP server that is being used by mid to large size companies. The FBI reports many VOIP systems are being compromised so criminals can sell minutes and leave the bill with the victim. But that's not my major concern.

The VoIP system marries the IP network with the old-style phone network (SS7). The latter has not been accessible to hackers on an easy basis prior to the VoIP deployments. By compromising a VoIP server, an attacker now has the ability to inject bad messages in the phone network. One may ask, what would that do: The most disastrous consequence can be bringing down the old phone network.

A crash that happened in 1990 brought down a phone system for 9 hours

<http://www.cs.berkeley.edu/~nikitab/courses/cs294-8/hw1.html>

Although the 1990 outage was not due to a cyber attack, such an attack is feasible in the near future by controlling a VoIP server.

(Rohit Dhamankar, senior manager of security research at TippingPoint)

A June article in Information Week, tells just how big VoIP financial crime can be: VoIP Security Alert: Hackers Start Attacking For Cash (VoIP could become the newest opportunity for cyberthieves, with the recent arrest of a Miamian only the beginning.)

## **Web Exploits**

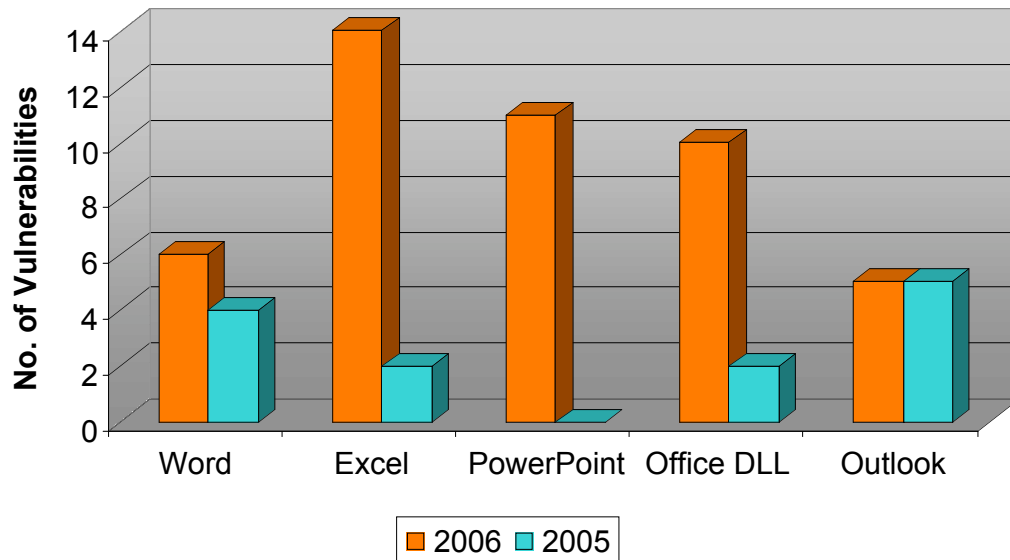
Web application vulnerabilities are so dangerous and wide spread because of the unique challenge they present to developers. Most traditional corporate application are hidden deep inside a data center behind multiple firewalls. Not so web applications. Customers need to have direct and fast access. As a result, many of the traditional protections like firewalls are of limited use. On the other hand, for the web application to be useful, it requires access to some of the companies most valuable data. The only thing that separates a hacker from access to this data is the diligence of the web developer who coded the respective application. Needless to say that given the complexity of these application and the time pressure to release them, mistakes are made. Best practices and code review techniques are still being developed for the tools and languages used in web development.

(Dr. Johannes Ullrich, Chief Technology Officer, SANS Internet Storm Center)

## Microsoft Office Vulnerabilities

In 2006, vulnerabilities in MS Office tripled as compared to what we witnessed the previous year. This is part of a continuing trend in Client-Side vulnerabilities which are flaws in client applications, client libraries and DLLs. About 45 serious and critical vulnerabilities were discovered in MS Office products alone. Among them 9 were zero day vulnerabilities in which an exploit or a worm was actively making use of the flaw and no patch was available.

### Microsoft Office Vulnerabilities



In a typical exploit scenario, a user opens malicious Word or excel document received via e-mail. Even more dangerous is a web based scenario where users browse the Internet and may come across malicious content which exploit vulnerable client-side components and can pretty much take control of the user's computer. Malicious web content can be embedded in a simple PowerPoint presentation or a JPEG image and may go completely unnoticed.

Prevalence of MS Office, limited preventive action against web-based attack scenario and high exploitation impact put these vulnerabilities on our TOP 20 list.

(Amol Sarwate, Manager, Vulnerability Management Lab, Qualys)

## **"Massive and still increasing exploits of vulnerabilities in web applications"**

Over the past several years, many business and government agencies web-ified their services, with a massive rise in e-commerce sites, on-line banking, and electronic government. Unfortunately, this rush to the convenience and lower cost of web-based transactions has brought with it massive vulnerabilities, particularly SQL injection and Cross-Site Scripting flaws. In recent months, the number of these flaws in web applications has shot dramatically upward. With SQL injection, an attacker can provide user input to trick an application into running unauthorized queries against its back-end database. This tactic has been used to steal multiple millions of credit cards in several high-profile hacking incidents. With SQL injection, an attacker can gain complete control of a database, stealing or altering its contents at will. What's more, with numerous information thefts logged in the past several years, cyber criminals have established a vast archive of information they can use years down the road for identity theft attacks. The other major web vulnerability is Cross Site Scripting, an attack that involves improper filtering in a web application. By providing user input that includes a browser script into the vulnerable application, an attacker can cause code to run inside of other users' browsers, stealing their sensitive cookies or, worse yet, engaging in transactions as that victim user. In our organization's penetration testing operations, we discover SQL injection flaws in approximately 40% of the applications we analyze, and Cross-Site-Scripting flaws about 80% of the time."

(Ed Skoudis, SANS "Hacking Exploits" Course Director and Senior Security Analyst, Intelguardians)

**Surge in zero-day vulnerabilities and attacks that go beyond Internet Explorer to target other Microsoft software.**

**Rapid growth in attacks exploiting vulnerabilities in ubiquitous Microsoft Office products such as PowerPoint and Excel.**

A zero-day vulnerability is a known flaw in software that does not have a patch available. Nearly every newly discovered vulnerability starts off this way, and in most cases a patch is available before the general public is made aware of the flaw. In 2006 we've seen a significant rise in attacks that take advantage of zero-day vulnerabilities, leaving a user or system unable to defend against the attack since no patch is available. The focus of most of these attacks is Microsoft products, in particular Internet Explorer. This has led to a widespread drop in the usage of the popular web browser and an increase in the use of other browsers such as Firefox, Opera, or Safari. Additionally, other Microsoft products such as Word and PowerPoint became targets used in very successful zero-day attacks over the past year. In fact, a vulnerability in the Windows graphical device interface (.wmf files) was the first zero-day attack of 2006.

This type of application-level attack is very hard to prevent with traditional flow-based schemes such as IDSs and firewalls. Likewise, consumer-oriented security solutions such as anti-virus software usually cannot detect the initial outbreak of a zero-day exploit attack. This fact is well known to the criminal and espionage communities, and is one of the key reasons for the rapid growth in this attack methodology. Many zero-day attacks that target Microsoft products are initiated in China. There are various theories about why China is such a hotbed for zero-day attacks, but most likely it is the fact that much of Microsoft's source code is available there with little intellectual property rights restriction on distribution, the culture supports reverse-engineering of proprietary code and research into exploiting code vulnerabilities, and there are few law enforcement investigations into the crews launching the attacks against targets in other countries.

(Marc Sachs, Director, SANS Internet Storm Center, and SRI International)