



For questions

Alan Paller, Director of Research, the SANS Institute (apaller@sans.org, 301-951-0102 x108)

Rohit Dhamankar, Project Manager, the SANS Top 20, and Senior Manager of Security Research, TippingPoint (rohitd@tippingpoint.com)
Other experts for comment listed at the end of this announcement

=====

SANS Top 20 Internet Security Risks of 2007 Point to Two Major Transformations in Attacker Targets

The cyber arms race continues. Cyber criminals and cyber spies have shifted their focus again, successfully evading the countermeasures that most companies and government agencies have worked for years to put into place. Facing real improvements in system and network security, the attackers now have two new prime targets that allow them to evade firewalls, antivirus and even intrusion prevention tools: users who are easily misled and custom-built applications. This is a major shift from prior years when attackers limited most of their targets to flaws in commonly used software.

=====

Scenario 1: The Chief Information Security Officer of a medium sized, but sensitive federal agency learned that his computer was sending data to computers in China. He had been the victim of a new type of spear phishing attack highlighted in this years' Top 20. Once they got inside, the attackers had freedom of action to use his personal computer as a tunnel into his agency's systems.

Scenario 2: Hundreds of senior federal officials and business executives visited a political think-tank web site that had been infected and caused their computers to become zombies. Keystroke loggers, placed on their computers by the criminals (or nation-state), captured their user names and passwords when they signed on to their personal bank accounts, and their stock trading accounts and their employers' computers, and sent the data to computers in different countries. Bank balances were depleted; stock accounts lost money; servers inside their organizations were compromised and sensitive data was copied and sent to outsiders. Back doors were placed on some of those computers and are still there.

Scenario 3. A hospital's web site was compromised because a web developer made a programming error. Sensitive patient records were taken. When the criminals proved they had the data, the hospital had to choose between paying extortion or allowing their patients' health records to be spread all over the Internet.

Scenario 4. A teenager visits a web site that exploits the old version of her media player that she never updated. She didn't do anything but visit the site; the video started up automatically when the page opened.

The attacker put a key stroke logger on her computer. Her father used the same computer to access the family bank account. The attackers got his user name and password and emptied his bank account (the bank

reimbursed him). US law enforcement officials followed the money and found that it ended up in an account being used by a terrorist group that recruits suicide bombers.

All of these scenarios are composites of actual events. To protect the victims from more embarrassment, facts have been altered and segments of multiple attacks have been combined. Thousands of attacks like these are happening every month. More than ten million computers have been compromised.

On November 27, the SANS Institute will unveil the 2007 Top 20 Internet Security Risks, the research group's seventh annual update of its consensus list of the cyber security risks that caused the most damage to individuals, corporations and government agencies in 2007. Forty three security experts from government, industry and academia in a half dozen countries cooperated to produce the consensus. Their names are listed in the Top 20 which is available online at www.sans.org/top20.

This year's SANS Top 20 illuminates two new attack targets that criminals have chosen to exploit and the older targets where attackers have significantly raised the stakes. Although the Top 20 focuses on emerging attack patterns, the old vulnerabilities are still being targeted by automated attack programs constantly scanning the web for vulnerable systems. So many automated programs are searching for victims that SANS Internet Storm Center (an early warning system for the Internet) reports that computers can expect to survive only five minutes before being attacked and will withstand the attacks only if they are configured securely before being connected to the Internet.

A summary of the highlights of year's Top 20, along with the most effective defenses, is attached at the end of this document.

"For most large and sensitive organizations the newest risks are the ones causing the most trouble," says Alan Paller, Director of Research at SANS. He goes on to say, "the new risks are MUCH harder to defend; they take a level of commitment to continuous monitoring and uncompromising adherence to policy with real penalties, that only the largest banks and most sensitive military organizations have, so far, been willing to implement."

According to Paller, web application insecurity is particularly troublesome because so many developers are writing and deploying web applications without ever demonstrating that they can write secure applications. Most of their web applications provide access to back-end databases that hold sensitive information. Says Paller, "Until colleges that teach programmers and companies that employ programmers ensure that developers learn secure coding, and until those employers ensure that they work in an effective secure development life cycle, we will continue to see major vulnerabilities in nearly half of all web applications." [On November 20, 2007, the Secure Programming Council released the first standard of due care for the security knowledge and skills that web programmers should be able to demonstrate. Interested parties can see the report at http://www.sans-ssi.org/essential_skills_java.pdf]

This year's top 20 project was led by Rohit Dhamankar, senior manager of security research for TippingPoint, the company that understands the attack vectors because they make intrusion prevention systems trusted by many of the most sensitive enterprises. According to Dhamankar, "Although half the total vulnerabilities reported in 2007 are in web applications, it's only the tip-of-the-iceberg. These data exclude

vulnerabilities in custom developed web applications. Compromised websites provide avenues for massive client-side compromises via web browser, office documents and media player exploits. This vicious circle of compromise is proving to be harder to break each day".

Data On How Big The Problem Is

Qualys, the firm that scans for vulnerabilities on millions of systems in hundreds of large organizations around the world, has an excellent perspective on where new vulnerabilities are being discovered. "We have seen a huge jump in the vulnerabilities in Microsoft Office products," says Amol Sawarte, Manager of Vulnerability Labs at Qualys. These charts show growth of nearly 300% from 2006 to 2007, primarily in new Excel vulnerabilities that can easily be exploited by getting unsuspecting users to open Excel files sent via email and instant message..

When systems are compromised through any of the new attack targets, spyware infections (including keystroke loggers) are among the most common result. Webroot, the largest spyware detection and monitoring firm, keeps track of how spyware is spreading. Gerhard Eschelbeck, Chief Technology Officer of Webroot reports that: "Since January 2007, Webroot has seen a 183 percent increase in Websites harboring spyware. (2) Infection rates for Spyware and Trojans that steal keystrokes are currently at 31 percent and rapidly growing, (3) Based on a small and medium size enterprise survey we conducted in September 2007 seventy-seven percent said their success depends on the Internet, and 47.2 percent reported lost sales due to spyware."

The Top 20 will be presented to the public in a meeting in London on November 28, jointly sponsored by SANS and the UK CPNI (Centre for Protection of National Infrastructure), where 200 leading UK security practitioners will gather to learn about the Top 20 and discuss countermeasures. The meeting, at 1700 UTC, is open to the press.

Free testing tools

As in past years, Qualys is making available a free service that tests computers for the elements on the Top 20 amenable to such testing. That service can be accessed at <https://sans20.qualys.com> .

This year, Applicure Technologies, a web application firewall firm, is offering a free monitoring tool that assesses how many web attacks are hitting IIS and Apache servers. It is available at www.applicure.com/?page=Sans.

About SANS

SANS is the most trusted and by far the largest source for information security training and certification in the world. More than 65,000 security professionals were trained by SANS. SANS also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS was established in 1989 as a cooperative research and education organization. Its programs now reach more than 215,000 security professionals around the world. Through SANS, a range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

Security Experts who can comment on the Top 20
Alan Paller, Director of Research, the SANS Institute (apaller@sans.org,
301-951-0102 x108)

Rohit Dhamankar. Project Manager, the SANS Top 20, and Senior Manager of
Security Research, TippingPoint (rohitd@tippingpoint.com)

Mark Osborn, UK CPNI (marko@cpni.gsi.gov.uk)

Plus:

(Active attacks) Johannes Ullrich, CTO, SANS Internet Storm Center
(jullrich@sans.org)

(Active attacks) Marcus Sachs, Director SANS Internet Storm Center and
Verizon (marc@sachs.us)

(Hacker exploits) Ed Skoudis, Founder, Intelguardians, and Course
Director SANS Incident Handling and Hacker Exploits
(ed@intelguardians.com)

(Spyware) Gerhard Eschelbeck, CTO Webroot (gerhard@eschelbeck.com)

(Vulnerability patterns) Amol Sarwate, Qualys (asarwate@qualys.com)

The SANS 2007 Top 20 Internet Security Risks, An Overview

Top New Risks That Are Particularly Difficult To Defend:

1. Critical vulnerabilities in web applications enabling the web site to
be poisoned, the data behind the web site to be stolen, and other
computers connected to the web site to be compromised.

Best defenses: Web application firewall, web application security
scanner, application source code testing tools, application penetration
testing services, and most importantly a formal policy that all
important web applications will be developed using a valid secure
development life cycle and only by developers who have proven (through
testing) that they have the skills and knowledge to write secure
applications.

2. Gullible, busy, accommodating computer users, including executives,
IT staff, and others with privileged access, who follow false
instructions provided in spear phishing emails, leading to empty bank
accounts, compromise of major military systems around the world,
compromise of government contractors, industrial espionage and much
more.

Best defenses: This is the most challenging risk. Security awareness
training is important but is definitely not sufficient to solve this
problem. Two defenses seem promising: (a) inoculation - in which all
users are sent periodic spear phishing emails that are benign. Those
who err are educated or cut off, (b) Admit that this problem cannot be
solved in all cases and establish new monitoring and forensics systems
that constantly search network traffic and systems for evidence of deep
penetration and persistent presence.

Other Priorities That Have Grown In Importance but Have Reasonable
Technical Defenses:

3. Critical vulnerabilities in software on personal computers inside and
outside enterprises (client-side vulnerabilities) allowing these systems
to be turned into zombies and recruited into botnets and also allowing
them to be used as back doors for stealing information from and taking
over servers inside large organizations.

- Web Browsers

- Office Software
- Email Clients
- Media Players

Best defenses: firmly enforced secure configurations (at installation time) for all applications, constantly verified patching and upgrading of both applications and system software, constant vulnerability scanning and rapid resolution of problems found, tightly configured firewalls and intrusion prevention systems, up-to-date anti-virus and anti-spyware at gateways as well as on desktops.

4. Critical vulnerabilities in the software and systems that provides the operating environment and primary services to computer users (server side software)

- Windows Services
- Unix and Mac OS Services
- Backup Software
- Anti-virus Software
- Management Servers
- Database Software
- VOIP servers

Best defenses: (mostly the same as group 3) firmly enforced secure configurations (at installation time) for all applications, constantly verified patching and upgrading of both applications and system software, tightly configured firewalls and intrusion prevention systems.

5. Policy and Enforcement Problems that allow malware to do extra harm and that lead to loss of large amounts of data

- Excessive User Rights and Unauthorized Devices
- Unencrypted Laptops and Removable Media

Best defenses: no-exception policies, constant monitoring, substantial penalties for failure to comply.

6. Application abuse of tools that are user favorites leading to client and server compromise, loss of sensitive information, and use of enterprise systems for illegal activity such as serving child pornography

- Instant Messaging
- Peer-to-Peer Programs

Best defenses: use only tightly secured versions of these tools, or prohibit them entirely.

7. Zero-day attacks

Best defenses: Build much more restrictive perimeters with "deny-all, allow some" firewall rules and redesign networks to protect internal systems from Internet-facing systems

=====
The BOTTOM LINE: WHAT IS NOT BEING DONE TO PROTECT SYSTEMS?

Best Practices for Preventing Top 20 Risks

- 1) Configure systems, from the first day, with the most secure configuration that your business functionality will allow, and use automation to keep users from installing/uninstalling software
- 2) Use automation to make sure systems maintain their secure configuration, remain fully patched with the latest version of the software (including keeping anti-virus software up to date)
- 3) Use proxies on your border network, configuring all client services

- (HTTP, HTTPS, FTP, DNS, etc.) so that they have to pass through the proxies to get to the Internet
- 4) Protect sensitive data through encryption, data classification mapped against access control, and through automated data leakage protection
 - 5) Use automated inoculation for awareness and provide penalties for those who do not follow acceptable use policy.
 - 6) Perform proper DMZ segmentation with firewalls
 - 7) Remove the security flaws in web applications by testing programmers' security knowledge and testing the software for flaws.

In other words, trust but verify through automation and testing.

=====

==end==