



FOR IMMEDIATE RELEASE

MEDIA CONTACTS:

Jennifer Lake
TippingPoint
+1 512-681-8111
jlake@tippingpoint.com

Jason Morris
Schwartz Communications for Qualys
+1 415-512-0770
qualys@schwartz-pr.com

Alan Paller
SANS Institute
+1 301-229-0777
apaller@sans.org

Top Risks Report Provides Unprecedented View of Security Attacks and their Business Threats

Experts from TippingPoint, SANS Institute and Qualys Present Data Tying High Profile Security Incidents with Specific Vulnerabilities

AUSTIN, TX – September 15, 2009 – A new bi-annual report from security experts [TippingPoint](#), [SANS Institute](#) and [Qualys](#) highlights the most significant attacks over the last six months, as well as the vulnerabilities these attacks exploit and how they can harm business. The report shows that many businesses are still extremely vulnerable to security attacks that can damage brand reputations and business operations. It helps businesses to review their defenses and ensure networks are up to date and able to quickly respond to today's emerging attacks.

Security attacks are growing in quantity and frequency, as well as becoming more impactful to business operations. With so many different types of security attacks targeting the enterprise, it is becoming difficult for organizations to see which threats pose the greatest risk. This report uses current data from appliances and software in thousands of targeted organizations to provide an accurate view of the attacks and the vulnerabilities they exploit.

“By combining information on attacks with data on specific vulnerabilities, we can provide organizations with real, actionable information for protecting their systems,” said Alan Paller, director of research for the SANS Institute. “Our goal in releasing this is to give overwhelmed security professionals the tools they need to prioritize their resources and security practices to achieve the best protection for their network.”

Key findings of the Top Risks Report include:

- **Unpatched popular client-side applications put businesses at risk for data theft:** PC applications often remain unpatched, compromising these machines to be used to propagate attacks and compromise internal computers. This leaves a window open for hackers to steal critical data, impact network performance and affect business continuity. Examples of these applications include Adobe Acrobat Reader, Microsoft Office and Apple QuickTime.

- **The number of Web application attacks is increasing, elevating the threat posed by previously trusted Web sites:** Web applications comprise more than 60 percent of the total attack attempts occurring on the Internet. These vulnerabilities are being exploited widely to convert trusted Web sites into malicious servers serving client-side exploits.
- **Operating system vulnerabilities are decreasing, but still pose a significant threat to an organization's security resources:** Operating systems (OS) have a lower number of vulnerabilities that can be remotely exploited to become massive Internet worms. The Conficker/Downadup is the exception and represents a major hole in many organizations' security strategy. Attacks on Microsoft OS were dominated by Conficker/Downadup worm variants. For the past six months, over 90 percent of the attacks recorded for Microsoft targeted the buffer overflow vulnerability described in the Microsoft Security Bulletin MS08-067.
- **A growing number of vulnerability researchers is causing a backlog of unpatched software and a greater risk that these will be exploited.** The number of people discovering zero day vulnerabilities is growing fast, yielding a growing number of vulnerabilities that remain unpatched – some for as long as two years. This lag time in patching increases the chance of hackers creating exploits targeting those vulnerabilities.

“The security attacks we describe in this report pose the highest risk for disrupting business operations,” said Rohit Dhamankar, director of TippingPoint's DV Labs security research team. “For organizations, understanding these attacks and how they exploit the vulnerabilities inherent in the network is a critical first step in building an effective security strategy.”

“The aggregate data in this new Top Risks report from the SANS Institute, TippingPoint intrusion prevention systems and Qualys vulnerability statistics enabled us to produce a new level of reporting with a more comprehensive picture of the state of Internet security,” added Wolfgang Kandek, CTO of Qualys and author of the Laws of Vulnerabilities. “This initiative underscores the importance of collaboration to fight the increased sophistication of attacks and helps business respond faster to new emerging threats”

In addition to identifying security risks, this report also provides recommendations for mitigating these threats. One of the report's most valuable insights discusses the *Twenty Critical Controls for Effective Cyber Defense*, which were released a few weeks ago. These controls gather the best practices from renowned security researchers. This report will map these controls to the specific vulnerabilities discussed.

Interested parties can download the full report at www.tippingpoint.com/toprisks or from SANS Web site at <http://www.sans.org/top-cyber-security-risks/>. Additionally the SANS Institute will be hosting a press conference on Tuesday, September 15 at 12:00 p.m. EDT. To join the conference, please dial: +1-312-878-3000 and type in pass code: 6573629.

About SANS Institute

SANS is the most trusted and by far the largest source for information security training and certification in the world. It 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 also sponsored the creation of GIAC, a leading industry security certification. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. 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.

About Qualys

Qualys, Inc. is the leading provider of on demand IT security risk and compliance management solutions – delivered as a service. Qualys' Software-as-a-Service solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures.

The QualysGuard® service is used today by more than 3,500 organizations in 85 countries, including 40 of the Fortune Global 100 and performs more than 200 million IP audits per year. Qualys has the largest vulnerability management deployment in the world at a Fortune Global 50 company.

Qualys has established strategic agreements with leading managed service providers and consulting organizations including BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, SecureWorks, Symantec, Tata Communications and TELUS. For more information, please visit www.qualys.com.

About TippingPoint and 3Com

[TippingPoint](#) is the enterprise security brand of 3Com Corporation (NASDAQ: COMS), a \$1.3 billion global enterprise networking solutions provider that sets a new price/performance standard for customers. 3Com has three global brands—[H3C](#), [3Com](#), and [TippingPoint](#)—that offer high-performance networking and security solutions to enterprises large and small. The H3C enterprise networking portfolio—a market leader in China—includes products that span from the data center to the edge of the network, while TippingPoint is a leading global provider of comprehensive network security solutions that address the security and regulatory compliance needs of complex network environments for enterprises, government agencies, service providers and academic institutions to deliver in-depth, no-compromise application, infrastructure and performance protection.

Copyright © 2009 3Com Corporation. 3Com, TippingPoint, and H3C are registered trademarks of 3Com Corporation or its wholly owned subsidiaries in various countries throughout the world. All other company and product names may be trademarks of their respective holders.