Information Security Predictions for the New Year

Submitted by: Marylebone Media Relations
Tuesday, 31 December 2002

TruSecure Expert Forecasts Virus and Worm Outbreaks and Trends for Early 2003

31st December 2002 - In the year 2002, corporations and organisations were spared most of the high-cost malicious code exploits prevalent in 2001, such as Nimda and Code Red although companies that relied on anti-virus software and did not filter email properly dealt with numerous attacks. TruSecure's technical director of malicious code research, Roger Thompson reports that in 2003, we may see the end of standard mass mailing worms. However, security professionals may want to brace for another attack in the class of and level of Code Red. Thompson's predictions for early 2003 include:

More Remote Access Trojans (RATs) or backdoors; overall, these attacks increased in 2002 but have decreased in the last few months. This type of security breach remains a favourite of the hacker community: malware code writers will continue to disguise RATs and backdoor scripts as "adult" movies and then post them to pornography new groups targeting inexperienced users. Expect them to continue through 2003 but they will be mixed with more and more greyware (i.e., spyware and advertising monitoring that is barely legal).

Mass-mailing Win32 viruses were largely unsuccessful in hitting corporations in 2002, with the notable exception of organisations that did not filter properly. One of the two biggest worms of the year was W32/Klez, which has been infecting home environments. The impact of the mass-mailing worm is mostly over for corporations but, in 2003, it will still have an impact on SOHO environments.

In 2001, Code Red was the most interesting piece of malware, with four versions and two separate code bases. In 2002, the Scalper/Slapper worms were in this category but were not as successful as Code Red. SqlSpida was successful at finding weak sQL servers but did not make it past the server into the organisation. Thompson expects another attack in 2003 in the class and level of Code Red.

W32/Nimda v1.0 was the biggest, most likely malware threat of 2002, but never hit. Given that Nimda was internally listed as v0.5 and knowing that the original worm didn't exploit all the known vulnerabilities in 2001, it is likely that there will be a v1.0 in 2003.

Macro and script viruses emerged at a rate of 200 to 300 a month in 2002 but this will dramatically decrease to only about 20 to 30 per month. Major anti-virus programs detect these and they will not have a measurable impact.

For media interested in speaking with Mr. Thompson, please contact Cynthia S. Smith of TruSecure Corp. at +001(703) 480-8509 or csmith@trusecure.com, or Sara Claridge of Marylebone Media Relations at 01344 876558 or sara@marylebone.co.uk.

About the Expert

Roger Thompson is director of malicious code research for TruSecure Corporation, where he monitors emerging threats and risks posed by the latest malicious code, whether viral or trojan. He provides

TruSecure's independent ICSA Labs with high-level guidance on malicious code certification standards and criteria, and is the principal developer of TruSecure Corporation's TruSecure Census toolset. Thompson joined ICSA Labs as director of Anti-Virus Research in June of 1997 and shortly thereafter chose to focus specifically on the growing threat of malicious mobile code. Each day, Thompson exchanges information with other anti-virus specialists around the world and is a regular speaker at security conferences both in the US and abroad. He is also on the editorial board of Virus Bulletin and the Advisory Board of the Wild List Organization.

About TruSecure

TruSecure is a leading security services provider, offering the only fully integrated, enterprise risk management services on the market. TruSecure's unique blend of proactive risk reduction with real-time security management, monitoring and response assures continuous security of critical business information assets. TruSecure Certification has become a globally recognised symbol of commitment to effective information security in an interconnected economy. Additionally, TruSecure owns the independently operated ICSA Labs® and Information Security® magazine. Headquartered in Herndon, VA, TruSecure protects more than 700 sites worldwide, with operations in North America, Central America, Europe and Asia Pacific. For more information about TruSecure Corporation, visit
http://www.TruSecure.com

Contacts:

Cynthia S. Smith

TruSecure Corporation

+ 1 (703) 480-8509

csmith@trusecure.com

Sara Claridge

Marylebone Media Relations

01344 876558

sara@marylebone.co.uk