“I told you so” is not exactly the favorite comment for anyone to hear, but unfortunately sometimes it has to be said.

ScanSafe <http://www.scansafe.com> starts its 2008 Annual Global Threat Report <http://www.scansafe.com/annualglobalthreatreport2008>, which as usual is available free through registration, with these depressing comments:

“In the ScanSafe 2007 Annual Global Threat Report, we predicted that Web surfers might be in for a wild ride in 2008. Unfortunately, we were correct. The year launched with wide-scale attacks on mom-and-pop style websites. These attacks persisted throughout 2008, but their volume was quickly overtaken by surges in SQL injection attacks, which were carried out via automated attack tools delivered via botnets. The success of the SQL injection attacks has been such that in July the rate of Web-delivered malware was higher than the entirety of 2007. And the rate in October 2008 was 21% greater than July.”

The Report explains that the study “…is an analysis of more than 200 billion Web requests processed in 2008 by the ScanSafe Threat Center on behalf of the company's corporate clients in over 80 countries across five continents.” The authors, including ScanSafe Senior Security Researcher Mary Landesman, comment, “The ScanSafe Global Threat Report provides a view of the threats which businesses actually face, rather than those experienced in labs or other artificial environments. Our data is gathered from real-time analysis by our proprietary threat detection technology, Outbreak Intelligence™ (OI) of every single Web request processed by ScanSafe in 2008. This approach differs from traditional methods of gathering information on Web-based threats, such as those methods afforded by distributed 'honeypot' networks. The artificial and contrived nature of honeypots, Web crawling, or similar technologies can lead to a skewed vision of the Web threat landscape which does not reflect actual user experience.”

Key findings from this year’s report:

- There’s been roughly a three-fold increase in malware being delivered via the Web from the start to the end of 2008.
- About a fifth of all the malware detected and blocked by ScanSafe was a zero-day malware threat.
- SQL injection and other attacks on Web sites grew from about 10% of the Web malware blocks at the start of 2008 to around 50% of Web malware blocks. The authors explain that these are serious problems for users: “Today’s compromised website is typically outfitted with invisible iframes or external source references that pull malicious content (generally malicious javascript) from attacker-owned domains. Those scripts are rendered by the Web surfer’s browser when they visit the compromised site. Outwardly, the compromised site appears perfectly normal – so much so that without careful and continual checking, the website owner may be oblivious to the threat their site is now
delivering to visitors.”

- “Indeed, as a result of the continuing mass compromise of legitimate websites observed throughout 2008, the standard 'safe surfing' advice of avoiding unknown or non-trusted websites no longer applies. Today, it is the known trusted site that should be viewed as posing the greatest risk to Web surfers.”

- Looking at vertical industries, “the top five most at risk verticals were Energy & Oil, Pharmaceutical & Chemical, Engineering & Construction, Transportation & Shipping, and … the … Travel & Entertainment industry.”

- The Koobface Trojan tried to convince users of social-networking sites such as Facebook, MySpace and Bebo to click on links supposedly circulated by their friends. “Once infected, users were directed to contaminated sites when they tried to use search engines, putting them at risk for identity theft, among other things.” Although Koobface represented only 1% of the observed malware in the report, ScanSafe recommends, “Users can lower their risk for malware spread via social networking sites by avoiding ‘promiscuous friending’ – that is, avoiding adding users they don’t know as ‘friends’. Users should also avoid clicking on links in emails received unexpectedly, even if the email appears to be from someone you know.”

- In a demonstration of the dangers of wasting time on celebrity Web sites (no, that’s my opinion, not ScanSafe’s), visitors to the compromised ParisHilton.com site were at risk of being infected by a data-stealing Trojan that could “target personal banking information” on home systems or “intercept, redirect or tamper with http and network traffic” on business networks in addition to stealing data.

- A revealing study by ScanSafe showed exponential growth in the number of unique malware signatures being defined by signature-based antimalware scanners. In the decade between 1986 and 2006, one vendor released a quarter-million signatures – but between 2006 and the end of 2008, the vendor added three times that many new signatures in only two years.

The report provides details and additional insights in its 30 pages and I recommend it to readers.

* * *

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>