

## Wolf in sheep's clothing: the insider can be the malicious outsider

*SANS Top 20 launch, Westminster, London  
Wednesday, 15 November 2006*

The launch in London yesterday of this year's Annual Top 20 listing highlighted some startling trends. Predictably Zero Day Attacks have grown dramatically in significance evolving from being something to fear in theory to a chilling reality in many applications and there was a sharp rise in web-based attacks on databases using SQL injections. But much more remarkable was the appearance on the list for the first of human vulnerabilities.

As Alan Paller, Director of the SANS Institute, outlined organizations have traditionally spent time debating where to focus their security resource: outsiders vs. insiders – which posed the bigger threat? Now that insiders can actually be malicious outsiders this debate is irrelevant. Roger Cummings of NISCC referenced, attackers are now targeting people with full legitimate access. We have seen this in the recent example of the [Glasgow call centres](#), which were infiltrated by criminal gangs; their employees being coerced into leaking sensitive customer information.

Mark Oram, Deputy Director Threat Investigation and Response of NISCC, drew stark attention to the growing capacity and creativity of the malicious market. The message was clear: this top list of attacks cannot be dealt with by traditional technology alone. The human response needs to be sharp and focused, to counter attack profiles that are consistent with foreign states and with resources on an industrial scale.

The need to protect critical data – commercial information on deals and a company's intellectual property – is very clear.

Traditional techniques, such as audit and pattern-based detection, simply cannot cope with the speed and efficiency with which targeted attacks are now taking place – especially when they arise from within an organization.

The need for dynamic security countermeasures in this situation is now clear. It is only a combination of human effort and automated security measures that can address the new threat profile. In an environment where even patch management systems are being compromised, this becomes even more strongly the case. New countermeasures and tools are needed to support the new breed IT security guard – the intrusion analyst – who needs real-time business-level information to detect and foil targeted attacks. Furthermore, in this chaotic scenario - in which even apparently legitimate key holders can be suspect - the most effective tool is one which sits very close to the asset it is trying to protect and which can operate independently of the normal business functions.

Unique new technology, introduced by Oxford-based Secerno, uses breakthrough machine learning algorithms to allow security personnel to build up a rich, business-level understanding of how applications and users are accessing databases and to insist on database interactions conforming only to allowable behaviors.

This allows intrusion analysts immediately to see when access deviates from normality. For example, it may be appropriate for a legitimate user to access a few records a minute, but alerts would be triggered when he reads hundreds. This might signal a Trojan usurping their authentication rights to download the corporate database, or a disenchanted user filling his memory stick with the company data.

The Secerno approach works even for those attack strategies that have not been seen before – the growing breed of zero day attacks. This is because Secerno's technology, unconstrained by the limitations of the pattern matching of traditional techniques, alerts on **all** non-standard statements.

This is the only effective approach that spans the full attack space – from targeted external to malicious insider attacks, to SQL injections and other zero-day exploits.

It allows business to build up a rich pattern of understanding of how users and programs access critical corporate data assets and provides business-level alerts to intrusion analysts when spotting any abnormal behaviour. It allows organizations to evolve a deep understanding of the relations between humans and applications and to monitor continuously the pulse of access to their core business information assets.

But it is the human touch that provides hope that the corporation can get one step ahead of the malicious market. With tools such as these, the defender can be proactive about security responses against the ever-changing threat from the outsiders who have become dangerous insiders.

For the full SANS Top 20 list see <http://www.sans.org/top20/>.

If you would like to speak to a Secerno commentator, please contact:

Jane Folwell  
Folwell PR for Secerno  
Tel: +44 (0) 1344 845132  
Mob: +44 (0) 7950 033370