ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 July 2014

www.computerfraudandsecurity.com

Featured in this issue:

The threat from within: how to start taking internal security more seriously

On average, a total of about 1,200 internal security breaches occur in UK businesses every single day. In the US, the figure is over 2,500. Yet despite this, insider threats are not among organisations' top security priorities.

For IT managers, internal security is a lesser priority than data loss, despite the fact that the most common source of data loss is via employees. Why is that? François Amigorena of IS Decisions explains how the insider threat needs to be addressed with a combination of cultural and technological solutions.

Full story on page 5…

Change detection technology has changed – for the better

File Integrity Monitoring (FIM) is a fundamental factor in the overall fabric of security. That said, having a poorly configured and misused FIM solution is more dangerous than not having one at all.

The sad reality is that many organisations are simply flushing away their multi-million dollar investments – and at the same time putting data security and system compromise at risk. Mark Kedgley of New Net Technologies looks at how modern FIM systems can benefit the organisation if they are used correctly.

Full story on page 8…

The Snowden wasteland

Have the leaks of intelligence files by Edward Snowden left us all in a more tenuous state? This incident has highlighted how our ability to defend ourselves could be undermined by insiders.

It's not just intelligence agencies that are at risk: private organisations are also vulnerable. Calum MacLeod of Lieberman Software explains how every organisation needs to initiate and enforce an effective defence against the inappropriate use of privileged access.

Full story on page 11…

Major trojan-based bank fraud nets €500,000 for cyber-criminals in a week

Cyber-criminals who targeted a large European bank managed to steal more than €500,000 in just a week, according to Kaspersky Lab's Global Research and Analysis Team.

The campaign – dubbed 'Luuuk' – was uncovered when Kaspersky's experts discovered a command and control (C&C) server. Its control panel indicated evidence of a trojan program being used to steal money from clients' bank accounts via Man in the Browser (MITB) exploits. Transaction logs on the server also contained information

Continued on page 3…

Contents

…Continued froom front page
about what sums of money were taken from which accounts. All in all, more than 190 victims were identified, most of them located in Italy and Turkey. According to the logs, the sums stolen from each bank account ranged between €1,700-39,000.

The campaign was at least one week old when the C&C server was discovered. Two days later, the criminals removed every shred of evidence that might be used to trace them. However, experts think this was probably linked to changes in the technical infrastructure used in the malicious campaign rather than spelling the end of the campaign itself.

"Soon after we detected this C&C server, we contacted the bank's security service and the law enforcement agencies and submitted all our evidence to them," said Vicente Diaz, principal security researcher at Kaspersky Lab.

He added: "On the C&C server we detected there was no information as to which specific malware program was used in this campaign. However, many existing Zeus variations (Citadel, SpyEye, IceIX, etc) have that necessary capability. We believe the malware used in this campaign could be a Zeus flavour using sophisticated web injects on the victims."

Kaspersky's experts noticed a distinctive quirk in the organisation of the so-called 'drops' (or money-mules), where participants in the scam receive some of the stolen money in specially created bank accounts and cash out via ATMs. There was evidence of several different drop groups, each assigned different sums of money. One group was responsible for transferring sums of €40-50,000, another with €15-20,000 and the third with no more than €2,000.

"These differences in the amount of money entrusted to different drops may be indicative of varying levels of trust for each drop type," said Diaz. "We know that members of these schemes often cheat their partners in crime and abscond with the money they were supposed to cash. Luuuk's bosses may be trying to hedge against these losses by setting up different groups with different levels of trust: the more money a 'drop' is asked to handle, the more he is trusted."

The C&C server related to Luuuk was shut down shortly after the investigation started. It's possible this was linked to a combined operation between the UK's NCA, Europol, the FBI and US Department of Justice targeting a Russian cybercrime gang using the Gameover Zeus malware variant and Cryptolocker ransomware. However, it's likely the gang behind Luuuk will simply switch to a new malware family and C&C server in order to resume operations.

Europol and ENISA team up as cybercrime-fighting duo

The heads of the EU's ENISA – the European Network and Information Security Agency – and Europol have formalised a strategic co-operation agreement that will allow them to work more closely and exchange expertise as part of their fight against cybercrime.

The purpose of the agreement is to enhance co-operation between Europol, its European Cybercrime Centre (EC3) and ENISA in order to support EU Member States and EU institutions in preventing and combating cybercrime. The agreement does not cover the exchange of personal data.

In particular, the organisations plan to exchange specific knowledge and expertise, general situational reports and reports resulting from strategic analyses and best practice. They also plan to build greater anti-cybercrime capacity through training and awareness raising, with the aim of safeguarding network and information security at the EU level.

ENISA is part of the EC3 Programme Board and respectively EC3 is part of ENISA's Permanent Stakeholders Group which advises the ENISA director on its yearly work programme and priorities. ENISA and EC3 have always worked together to reinforce EU-level cyber-security and reduce cybercrime. Work so far has included: producing a joint paper on botnet mitigation; participating in European Cyber Security Month; exercises such as CyberEurope; producing a good practice guide for CERTs; and enhancing CERT/law enforcement co-operation through workshops and conferences.

Microsoft battles botnet – and accidentally takes down legitimate sites

Microsoft has once again taken to the courts in the fight against botnets. In this case, however, the legal action had unintended consequences.

The firm was successful in winning an injunction from a Nevada court that allowed it to assume control over a number of domain names, owned by the No-IP service, that were being exploited by botnet operators.

No-IP's dynamic DNS service – and many others like it – are used (quite legitimately) by people who want to use a fixed domain name that can direct people to a server whose IP address is subject to change. It seems, however, that botnet operators who are controlling 7.4 million infected Windows PCs are exploiting no-IP's domains to ensure that the compromised machines can contact their command and control servers.

Microsoft claimed that there were some 18,400 or so malicious hosts using (via sub-domains) the 23 domain names employed by No-IP. By taking control of the 23 domains, the plan was for Microsoft to filter out malicious traffic and pass on any legitimate packets. But according to No-IP, that's not what happened. The firm said that it reckoned there were only around 2,000 malicious hosts and that a very large number of legitimate users were having their systems blocked. No-IP also complained that Microsoft took action without consulting it, and that the response was out of proportion to the problem.

On a more positive note, Microsoft has launched what it calls "a security and threat information exchange platform for analysts and researchers working in cyber-security." Running on the Azure platform, Interflow is an automated, machine-readable feed of threat and security information that can be shared in near real-time, the firm says. The aim is to help security professionals respond more quickly to threats. Microsoft also hopes the new service will help reduce cost of security by automating processes that are currently performed manually.