If you have been forwarded this email and would like to be added to the distribution list, click here.

THE INKERMAN GROUP

INKERMAN FRAUD WEEKLY

Issue 3

Welcome to Issue 3 of the Inkerman Fraud Weekly, providing businesses and individuals with a weekly overview of global fraud and corruption activity, gathered and analysed by The Inkerman Group's experienced Private Investigations and Corporate Intelligence teams.

In this Issue

- IP Theft in China
- Chat Session Banking Trojans
- Hacking Threat
- Contact Us

BENCHMARK CASE FOR IP THEFT IN CHINA

In what is being billed as the largest intellectual property (IP) case to date in China, US energy company AMSC is taking on China's largest wind turbine manufacturer Sinovel Wind Group Co., amidst claims of copyright infringement, breach of contract and theft of trade secrets amounting to around US$1.2 billion. Understandably, due to China's questionable record on protecting foreign businesses' IP rights, the case is drawing a significant amount of international attention as companies worldwide are eager to see if the Chinese courts will rule in favour of the US company in a claim which many believe would be an "open and shut" case in the western judicial system. Beijing is apparently well aware of the international attention that the case has garnered and will not only be keen to try and suppress potential foreign investors' fears of becoming a victim of IP theft in China but to also shift the economy away from manufacturing and towards research and innovation, something which will require far more rigorous IP protection. A decision on the case is expected in the next few months.

CHAT SESSION BANKING TROJANS

Live chat sessions are being hijacked to trick business banking customers into providing their details to cyber criminals. The attack, which has been targeting businesses rather than consumers, is carried out through the Shylock malware platform and stalls the loading of the bank's webpage, displaying a security message to the user and transferring them to an "advisor." The hacker can then check the victim's banking details in real-time and, if valid, chat to them by posing as a bank employee to gather further information and entice them to verify the fraudulent transactions that the hacker is conducting. This follows reports of the Neloweg banking Trojan that detects websites visited and harvests users' details, particularly targeting banking websites. So far, this Trojan has been localised to Europe, with a particular focus on the UK and the Netherlands.

DDoS ATTACKS A SIGNIFICANT THREAT

A recent survey amongst IT directors in 300 medium to large sized businesses in both the US and UK has revealed some interesting trends in relation to Distributed Denial of Service (DDoS) attacks.

A DDoS attack makes a computer or network resource, such as a company's website unavailable by flooding or crashing the server with artificially high levels of internet traffic.

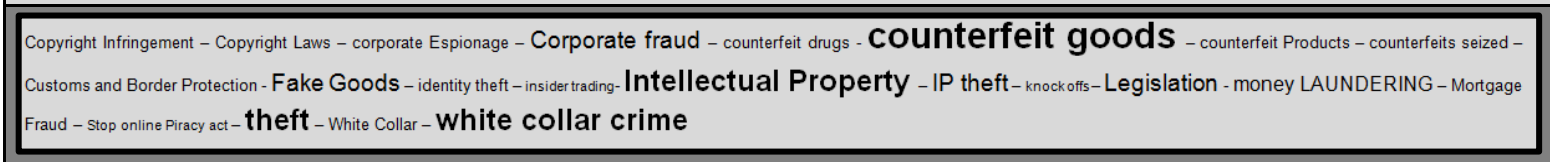
The report uncovered that around 31% of the organisations questioned had fallen victim to a DDoS attack in the last twelve months and that the US companies were nearly 20% more likely to be attacked in this manner.

This increased vulnerability also explains why 63% of US IT directors said they were concerned about the threat of DDoS attacks with only 29% of those in the UK expressing the same concerns.

Despite being committed for a number of reasons including political and financial motives, in the US, competitors were blamed for more than half of the attacks.

BUSINESSES NOT TAKING HACKING THREAT SERIOUSLY

On 01 March 2012, an FBI investigator warned that businesses are taking the threat of hacking "too lightly." 2011 was hailed as the year of hacking and 2012 looks likely to accelerate this trend, with a number of high-profile attacks against businesses, including Symantec, Foxconn and Combined Systems. The warning follows the arrest of twenty-five individuals associated with the hacking collective Anonymous on 29 February 2012. Though groups such as Anonymous cite political beliefs as the motivation for their attacks, it was warned that such groups can be hijacked by criminal elements for their own gain, and are therefore a high risk to businesses. Such attacks can have a devastating effect including loss of revenue, consumer confidence, intellectual property theft and breach of data protection law.



This tag cloud has been generated using specialist horizon scanning software and represents this week's most frequently reported fraud and fraud-related concepts across a variety of sources

CONTACT US

If you are concerned about fraud and need advice on pre-employment screening, due-diligence, private investigations or electronic sweeps, contact The Inkerman Group.

The international business risk and intelligence company.

The Inkerman Group – Operations Centre – Inkerman House – Ashford – Kent – TN23 1PF
investigations@inkerman.com – +44 (0)1233 646940 – www.inkerman.com

Click here to unsubscribe from this mailing list