

## SOCA Alert A9A202N



### Counter Corruption - Managing Insider Threats

This is Alert warning A9A202N issued by the Industry Exchange and Alerts Branch of the Serious Organised Crime Agency (SOCA). It is based on assessed intelligence, warns of dangers and threats from serious organised criminality and is devised with the aim of bringing about preventative or remedial action.



**SOCA**  
SERIOUS ORGANISED CRIME AGENCY



July 2009

## Counter Corruption – Managing Insider Threats

The story so far.....

**NEWS**

---

**GANG SENTENCED OVER £229 MILLION FRAUD!**

An investigation by the Serious Organised Crime Agency (SOCA), led to a 'lord of the manor' and his four accomplices facing jail sentences totalling 30 years for their roles in the attempted £229m theft from the London offices of the Sumitomo Matsui Banking Corporation (SMBC).

Helped by a corrupt employee of the bank, the thieves were able to gain entry and install 'key logging' software

in a bid to compromise the bank's payments system. Once retrieved, the gang used the information in an attempt to transfer vast sums of monies to a number of world wide accounts.

Luckily for the bank, staff were alerted when errors in the transfer process failed to send the payments, had this not happened the gang would have got away with the largest electronic bank heist in history.

### What we would like you to do

This Alert and good practice guide - **Protecting Business Assets**, is intended to act as a timely reminder of the increasing problem of insider corruption. Protecting business reputation and assets will be integral to your organisation. To help maintain standards of data protection we ask that you use this guide to complement your existing procedures.

The Alerts process is the way in which SOCA provides information to the private sector. To help us to improve this service, we would welcome any feedback you have on both the Alert itself and the information provided to you. Please email all feedback to [alerts@soca.x.gsi.gov.uk](mailto:alerts@soca.x.gsi.gov.uk) and include the reference **ALCMAEON** in the subject line.

This Alert is **Not Protectively Marked**, however SOCA requests that you comply with the handling instructions at the end of this document.

## Information Report

In October 2004, specialist investigators were called to the London offices of the Sumitomo Matsui Banking Corporation (SMBC) to investigate what appeared to be evidence of suspicious activity and possible hacking.

The investigation confirmed that the bank's security manager had facilitated the gang's entry into the building. Although the majority of cameras had been tampered with, the bank's CCTV system recorded the gang's exit from the building. Forensic analysis revealed that the gang had entered the bank and installed 'key logging' software on employees' computers to 'harvest' account data.

The gang later then used the bank's systems to make a number of electronic payments to offshore accounts. Thinking this had been successful, they then cut the network cables and formatted hard drives to obstruct detection and left. Fortunately for the bank, the gang had made errors on the electronic payment forms which meant that the transactions were not processed.

Investigators were able to identify and arrest the two criminals who were responsible for installing the key logging software and were able to trace and arrest other gang members through the accounts that were to be used to siphon off the funds. In 2009 the group received sentences which collectively totalled over 30 years imprisonment.

### Comment

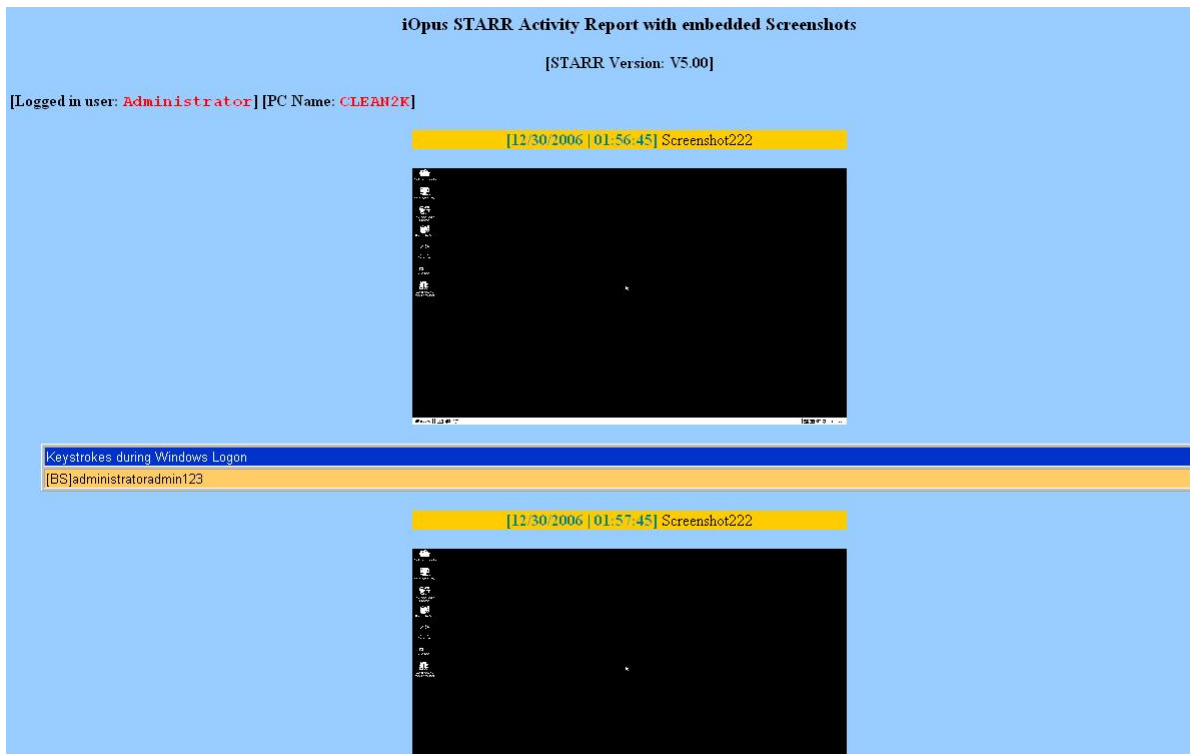
Fraud costs the UK £20 billion per year and employee perpetrated fraud represented more than a third of cases that went through the courts in 2008.<sup>1</sup> This not only affects an organisation's productivity, profits and reputation but has wider social and legal implications. With the current difficult economic conditions faced by businesses, any type of breach could put jobs at risk and incur heavy penalties for lapses in data management and security. Robust measures that are subject to constant review will ensure the best level of protection from criminals who are intent on attacking your business.

---

<sup>1</sup> KPMG Fraud Barometer 2008

This Alert is **Not Protectively Marked**, however SOCA requests that you comply with the handling instructions at the end of this document.

### Examples of 'key loggers'



Screenshot of the iOpus Starr software keylogger which was installed on the SMBC computers.



A 'key logger' variant



A USB port 'key logger' example as it would be plugged into the back of the computer.

This Alert is **Not Protectively Marked**, however SOCA requests that you comply with the handling instructions at the end of this document.

USB devices can be disguised in many ways; as toys and other apparently innocuous gadgets, and can be removed once installation has been successful. If this technique is used, audit may be possible but there will be no visible evidence of tampering.

Installation of malicious software, or 'malware', provides the installer with a further mechanism to steal information beyond the physical use of a USB-type device. When key logger technology is used on a computer it enables the perpetrator to see what has been typed. In some instances, devices are capable of detecting mouse clicks as well as key strokes so even those businesses which use virtual keyboards can be vulnerable.

Snapshots of captured information are then often automatically sent to the Trojan author via file transfer protocol (FTP).

It is difficult to detect key logger malware and often equally difficult to remove it once installed. It usually infects a system when images or music files are downloaded from the internet. However, there are a large range of readily available security products on the market designed to detect and delete such viruses, and most large company corporate systems are adequately ahead in this field.

To help you consider how you might respond to these types of threat we have compiled a short guidance document, entitled **Protecting Business Assets**. This document is attached to this Alert.

### *Disclaimer*

*While every effort is made to ensure the accuracy of any information or other material contained in this document, it is provided on the basis that SOCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or other material contained herein.*

*Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.*

© 2009 Serious Organised Crime Agency.

## Protecting this document

This is a government document that has been graded as **Not Protectively Marked**. The information contained herein is time sensitive and to maximize protection against the documented threat is deemed appropriate for wide dissemination. We do however request that you handle and manage this Alert in a considered way and dispose of it accordingly.

## Handling advice – Legal information

This information is supplied by SOCA in strictest confidence under authority of Section 33 of the Serious Organised Crime and Police Act 2005.

In accordance with Section 35(1) of the Serious Organised Crime and Police Act 2005, this information must not be disclosed by the recipient without express prior consent from SOCA. Therefore, do not pass on this document or any part thereof, or disclose any information contained in it, to any third party without the express prior written consent of SOCA.

In addition, if, because of this exercise you are able to provide any information to SOCA that you consider might be relevant to identifying or preventing crime, then we encourage you to do so. We would like to remind you of the provisions contained in Section 34 Serious Organised Crime and Police Act 2005. These provisions say that any information provided by you to SOCA, in order to assist SOCA to discharge its functions which include the prevention and detection of crime, will not breach any obligation of confidence which you may owe to any third party or any other restriction on the disclosure of information. S34 requires that disclosures of personal information about living individuals by you to SOCA must still comply with the provisions of the Data Protection Act 1998 (DPA), but you may be satisfied that disclosure by you of such personal information to SOCA in order to assist SOCA to prevent and detect crime is in deed permitted by the DPA. Please, therefore, submit all S34 information to [alerts@soca.x.gsi.gov.uk](mailto:alerts@soca.x.gsi.gov.uk).

This Alert is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and should not be disclosed in response to FOIA requests made under this Act.

Requests for disclosure under the provisions of the Data Protection Act 1998 or other legislation must be referred to the Industry Exchange and Alerts Branch of SOCA, by email to [alerts@soca.x.gsi.gov.uk](mailto:alerts@soca.x.gsi.gov.uk) or by telephoning 0207 238 8541.

## Alert Coloured Roundels

SOCA Alerts are marked with either a Red or Amber Roundel. This is designed to indicate the urgency of the warning. Red may indicate a more immediate or specific threat, whilst those marked Amber will provide more general information that may complement existing knowledge.

## SOCA Prevention and Alerts

Recognising that the private sector is often the victim of serious organised crime and is engaged in its own efforts to prevent, deter and frustrate criminal activity, SOCA Prevention and Alerts seeks to forge new relationships with business and commerce that will be to our mutual benefit – and to the criminal's cost. By issuing Alerts that warn of criminal dangers and threats, Prevention and Alerts seeks to arm the private sector with information and advice it can use to protect itself and the public. For further information about this Alert, please contact SOCA Industry Exchange and Alerts Branch by email [alerts@soca.x.gsi.gov.uk](mailto:alerts@soca.x.gsi.gov.uk) or by telephoning 020 7238 8541. For more information about the Serious Organised Crime Agency go to [www.soca.gov.uk](http://www.soca.gov.uk).