University of East Anglia

SYS CONSULTING

Security & Network Forensics

# Computer Network Forensics

## Business Challenge

Data centres have grown in scale and complexity over the past decade. Large organisations have data centres with thousands of servers hosting tens of thousands of applications. These large data stores become targets for criminals looking for credit card and commercially sensitive information for resale to organised crime gangs and terrorists.

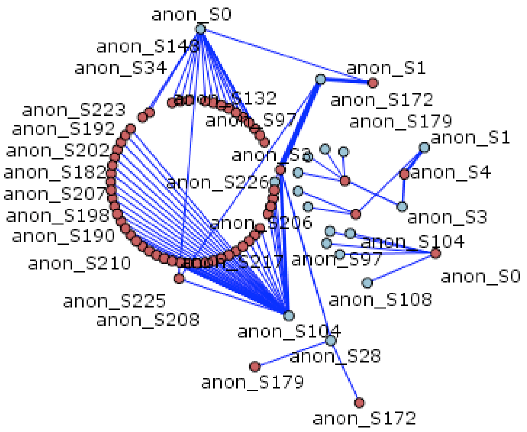
When a data centre has been breached the traditional forensic technique has been to take an image of each machine and analyse it looking for evidence. This process requires a skilled investigator to pick through the information machine by machine. This process is very time consuming and expensive and is impractical for large numbers of machines.

The problems the organisation face are how they can accurately identify all the machines that have been compromised, how much data has been stolen, the weakness in their security and to turn that information into actionable risk management decisions.

## Our Solution & Expertise

SYS Consulting has considerable experience developing data-mining techniques. New techniques have been developed to allow an investigator to examine the network flow information to identify the machines which the criminal has compromised. These techniques provide the only mechanism to identify all the machines the attacker has been in contact with other than by manual inspection of every machine. The speed with which an investigation can be conducted is also increased.

The techniques developed use data already being produced by the network equipment to provide a capability analogous to CCTV.  Activities can be tracked and the data can provide a complete picture of the activities on the network. A wide range of behaviours can be isolated and, depending on the problem, individuals can be identified.



For insider threats this wide ranging surveillance is vital. In the event of a conspiracy you want to identify as many conspirators as possible to avoid anyone slipping through the net and destroying evidence or making assets unavailable.

One of the major features of the technique is that the hacker cannot easily interfere with the collection of network data. A secure monitoring system significantly increases the chance of identifying the culprit and managing an incident. Working in collaboration with experts in the organisation we can detect “unwanted” behaviour on the network quickly and cost effectively.

## Business Benefits

These techniques and our skills provide the only cost effective way to understand large-scale network activity over an extended time period.

The ability for a business to understand what has actually happened and respond to an incident in a timely and effective manner can be the difference between the business surviving or failing.

The ability to block all the exploited holes in a network is vital to maintain the integrity, availability and confidentiality of information.