



Counterpane™
Internet Security

Counterpane Professional Services Case Study: Network Forensics Investigation

Description of Client: Large US Defense Contractor

Description of Problem: Client contacted Counterpane when they discovered they had been compromised by hackers coming from IPs originating from The People's Republic of China (PRC). They contacted the FBI who confirmed their findings and collected forensic evidence to identify the intruder's signature, but then recommended they contact a private company to perform the appropriate post-intrusion work and forensics to attempt to discover extent of the compromised hosts.

Details of SOW:

Scope: The overall scope of the engagement was to address any current security threats, and the creation of a roadmap for developing a robust, sustainable information security practice based on the ISO 17799 framework in order to improve the customer's security posture. This was amended once the overall scale of the intrusion was revealed to include leveraging the skills of four (4) senior information security consultants to act as subject matter experts in analyzing their recent security events. Additionally, two (2) senior information security consultants conducted forensics work.

Service types: The general professional services types used in this engagement were from the following categories:

- Threat Assurance Services
- Audit Compliance Services
- Due Diligence Service
- Brand Protection Services

Number of assigned personnel: Initially four personal, that number was increased to six to include two forensics experts

Timeline to Delivery: Due to the *post facto* nature of the engagement we were defining the time-line as we went along. As soon as the customer was in possession of our Statement of Work, they signed and told us to make an initial discovery, which lead to a change order to expand the nature of the engagement.

Findings: The customer had been overrun with a network worm that compromised the corporation's active directory and file servers. The worm was detected by finding changes to Microsoft's system's files (.exe and .dll). The worm searched for file types based on keyword searches and then copied the files and sent them to PRC via several intermediary cities. The worm spread throughout their network.

Recommendations: Determine the cost of the information compromised. Conduct forensics on their directory servers, mail servers, and file servers, rebuilding all compromised hosts. Institute basic security measures for the organization. Develop an internal set of policies and procedures to control IT deployment on their network and bring IT standards under a single authority.