Global Digital Forensics Case Study Drug Diversion

Case Type – Prescription Drug Diversion, Anti-Counterfeit, Brand Protection, International – Computer Forensics

Environment – On-Site Seizure at Several Locations Throughout the United States and Canada.

Industry – Pharmaceutical

Systems Involved – Desktops, Laptops, E-mail, Handheld Devices and Email.

Case Background

A Pharmaceutical Company began receiving complaints from its representatives in certain geographical areas that sales of normally high volume drugs were slowing down considerably. The companies internal security department as well as the security departments of its major distributors began an investigation. The results of the investigations led the security professionals to believe a significant amount of the companies product was being diverted from foreign countries into The United States and sold through smaller distributors who specialized in sales to locally, privately owned, pharmacies and dispensaries within nursing homes. The diversion activities were immediately reported to the local authorities in the regions as well as to the FDA.

An investigation was immediately launched and millions of dollars of diverted drugs and repackaging equipment was seized from several locations, including the warehouses of fully licensed pharmaceutical distributors. Along with the diverted product the computers and other electronic equipment was also seized.

The seizure went smoothly and the company was satisfied as were investigators from the FDA and local law enforcement however the case was severely hindered by the fact that the majority of communications between the principals of the distribution companies (foreign nationals) and the foreign suppliers was conducted by email. There were was also virtually no paper records on site. While the local authorities and the FDA had access to computer forensic labs both faced similar roadblocks in their investigations; the labs were severely backlogged and the systems were encrypted and fairly complex as well as being a foreign language.

Toll Free: 1-800-868-8189
Int. Phone: Phone 727-287-6000
http://www.evestigate.com

It became obvious that the investigation would be delayed until one of the labs cleared some high priority cases and could dedicate the time required to forensically analyze the computers from the seizure. Time was of the essence and everyone knew that the computer forensics had to begin immediately if the diversion was to cease and the case successfully prosecuted since the suspects claimed they were reshipping the drugs outside the US (a legal practice) and had shipping bills that appeared to back this statement up, without the documentation on the computers it was almost assured that the US attorneys Office would drop the charges.

GDF Involvement

The company called in GDF and working in cooperation with the local authorities as well as with the FDA and US attorneys office GDF was able to commence Computer Forensic Analysis of the computers seized at the pharmaceutical warehouses and provide the information and artifacts recovered during the computer forensic analysis to the US Attorneys Office.

GDF dispatched a Mobile Computer Forensic Lab and along with investigators from the US Attorneys Office created forensically sound copies of the hard drives seized from the warehouses to be used to conduct the computer forensic analysis. Strict chain of custody was maintained and the computer forensics were conducted under the supervision of the US Attorneys Office following all accepted computer forensic methodologies.

The Findings

GDF Computer Forensic Specialists were able to decrypt and extract a wealth of information from the systems that were forensically analyzed. By conducting a complete computer forensic analysis of all the data the hard disks contained GDF was able to provide documentation showing that the diverted drugs were being purchased from distributors in Europe and from Canada and being shipped to the US as what appeared to be legitimate transactions. The computer forensic analysis also showed that the distributor had purchased equipment to unwrap

Toll Free: 1-800-868-8189
Int. Phone: Phone 727-287-6000
http://www.evestigate.com

the foreign drugs as well as repackaging equipment, all signs of a legitimate drug repackaging and exporting company.

GDF's computer forensic analysts were also able to extract documents showing that the owners of the distributors also controlled several pharmacies in the area as well as several nursing home and ACLF facilities in the area all of which appeared to purchase drugs from the distributors. There were also many invoices for custom vitamins shipped to another distributor just two buildings away that also appeared to be controlled by the suspects.

The Outcome

Using the digital evidence the computer forensic specialists gathered along with the physical evidence the United States Attorney was able to prove:

1. The distributor was purchasing drugs from foreign sources to be sold within the United States.

2. The Distributors were engaged in drug diversion for over 10 years

3. The distributor was repackaging vitamins manufactured to appear the same as the prescription drugs and selling and shipping them to Asia.

4. The distributor was operating unlicensed pharmacies and nursing homes.

The company sustained over 13 million dollars a year in lost revenue and the suspects distributed millions of dollars in counterfeit drugs throughout Asia potentially endangering the lives of hundreds of innocent people.

The suspects were convicted and sentenced in the United States and being investigated in 5 other countries.

Toll Free: 1-800-868-8189
Int. Phone: Phone 727-287-6000
http://www.evestigate.com