B4 The Role of Global Telecommunications Providers in Tracking and Investigating Information Security Incidents

Christopher W. Day, BS, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131*

After attending this presentation, attendees will have a better understanding of how global telecommunications providers can provide assistance to digital forensic investigators investigating a host of information security breaches and incidents. Global providers have a vested interest in tracking and mitigating many forms of information threats such as so-called advanced persistent threats, organized crime activity, botnets, child pornographers, and so on. Many providers offer their customer base various services against these threats, while others are compelled by their national governments to maintain certain records for law enforcement use. All are interested in protecting their infrastructure from today's increasingly sophisticated threats. The types of information potentially available to those investigating an information incident may include extensive flow records (including multi-hop, multi-jurisdictional data), access logs, reputational statistics for IP blocks and addresses, peering data, and many others. In certain limited circumstances, even captured packet data may be available.

This presentation will impact the forensic community by providing practitioners with awareness of the types of information that may be available from global telecommunications providers, how the information can provide evidence to support an investigation, and how to go about requesting and preserving the evidence. There are also a number of formats in use today for reporting incidents as well as requesting support from a provider for an investigation. A number of case examples will be discussed to better demonstrate how the various types of data have been used in this study to investigate a wide array of computer intrusions and incidents in the past. Finally, various legal frameworks and privacy issues that come into play when requesting and utilizing this sort of information will be discussed. As well as a number of industry initiatives to capture, utilize, and normalize data submission. This useful data in an appropriate manner for investigation purposes while preserving and protecting privacy and civil liberties will be shared.

Many incidents today involve multiple systems in various international jurisdictions. Piecing together the evidence to not only understand the scope of the incident, but also determine attribution of the perpetrators, can be a daunting and time-consuming process. In many cases, investigators are not aware of what types of information may be available to them from a given provider. In some scenarios, access to a known-malicious host, in its entirety, has been made available for forensic analysis. In certain limited circumstances, even captured packet data may be available under the appropriate legal frameworks. Additionally, with the ever-growing movement of computing workloads into various cloud computing infrastructures, many owned and operated by telecommunications providers, investigators must be cognizant of what types of evidence and information cloud providers are maintaining to support their businesses and how that information can be useful to an investigation. The presentation will also discuss issues relating to the scale of the evidence acquisition problem brought about by increases in bandwidth, system memory, data storage, and the elasticity of today's cloud computing environments. Investigators must be prepared to receive and process potentially massive amounts of data (possibly on the order of terabytes) when requesting incident information from large providers.

Telecommunications, Global, Investigation

