Employee Theft Forensic Investigation: GLOBAL TECHNOLOGY COMPANY

Client challenge

After receiving a "cleaned" corporate laptop from an ex-employee a full month after she left to join a competing firm, a large, global software company was concerned she may have stolen enterprise intellectual property or violated her non-compete agreement. They needed a team of experts to examine the laptop to determine if evidence of these suspicions existed.

Crypsis solution

The company contacted The Crypsis Group to see if they could validate their suspicions. The Crypsis experts' initial review of the laptop's forensic image verified that most of the user activity, files, and programs had been deleted. But that was not the end of the story — applying their forensic expertise and using software tools developed for this purpose, the investigators recovered data from the computer's Volume Shadow Copy in addition to other deleted, but not yet overwritten, data. Most of the artifacts were almost completely intact and able to be analyzed.

Among the key findings, the team examined various forensic artifacts detailing network connection history and determined that the laptop had been connected to the ex-employee's new company network several days after she resigned.

Furthermore, the Crypsis investigators found evidence that multiple USB drives had been connected to the laptop after the suspect resigned but before she had turned in the laptop to the client, specifically while connected to the competitor company's network. Through forensic analysis, the team found that artifacts of numerous client-specific directories and files existed on, and were opened from, these USB devices while on the competitor's network and at other times after resignation, including marketing templates, user guides, code reviews, and rollout plans.

Finally, and perhaps most critically, were the considerable lengths to which the suspect went to mass-delete files and evidence of specific user activity on the laptop as she apparently sought to cover her tracks. Crypsis investigators found evidence that, prior to being returned to the client, the suspect installed and used TeamViewer software: proprietary software for remote control, desktop sharing, online meetings, web conferencing, and file transfer between computers. Piecing together information from various forensic artifacts, the Crypsis investigators discovered an incoming connection from an IP address that resolved to the remote location of one of the outsourced technicians that the suspect managed while she was at the client's firm. From these details, it was clear that mass deletions of files on the laptop took place during this TeamViewer session and immediately thereafter.

The data deleted contained synced email messages, including evidence the suspect conducted email conversations with the company's outsourced service providers that were likely in violation of the nondisclosure and noncompete agreements that those providers had signed.

AT A GLANCE

A global software company suspected an ex-employee of accessing intellectual property following her exit from the company — but all they had was a "cleaned" laptop she had in her possession for a month following her resignation. The Crypsis team investigated, using forensic tools and techniques, finding a trail of evidence.

RESULTS

Crypsis experts know that computers or other digital devices are rarely fully "wiped clean." Useful, actionable information is usually hidden somewhere in the system, and key data and files can often be swiftly recovered and examined.

By using host-based forensic analysis techniques, tools, and methodologies, the Crypsis investigative team was able to provide the client with evidence of potential theft of intellectual property, remote access, destruction of data, and attempts to solicit current employees — which could be in violation of the departing employee's contract, if not criminal law.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com