To Catch a Trade Secrets Thief – The Computer Forensics Way

IP Investigations and Protection

Trade Secrets Theft

NEW YORK, NY, UNITED STATES, March 2, 2021 /EINPresswire.com/ -- On January 13th, the FBI arrested a former medical director of a pharmaceutical company in New Jersey for allegedly stealing trade secrets.

Essentially, the accused transmitted proprietary information either to his personal email address, onto a USB drive, or to his new employer (another company that is a direct competitor of his former employer.)

This post will focus on the forensic computer investigation that uncovered the alleged illegal transfer of trade secrets.

> This post will focus on the forensic computer investigation that uncovered the alleged illegal transfer of trade secrets."
>
> *Ron Alvarez*

INSTRUCTIVE FOR INVESTIGATORS

The sixteen (16) page criminal complaint presents not just the details of the crime, but the fundamentals of the computer forensic investigation, which I think would be useful for investigators to have some familiarity with.

The New Jersey pharmaceutical company discovered the theft and notified the FBI after the accused left the company and went to work for a direct competitor.

Data Loss Prevention Basics

The company had in place an internal computer monitoring system, otherwise known as "Data Loss Prevention" (DLP),

Data Loss Prevention includes two (2) tools:

Network Data Loss Prevention (NDLP), that tracks employee email activity, and

Host Data Loss Prevention (HDLP), embedded in all company work computers.

As the complaint details, "The [accused'] company computers prompted a Security Group (SG) alert on both the NDLP and HDLP monitoring tools."

The DLP Tool had identified 106 company documents transferred from the accused's computer through a "web post" to his personal accounts.

A "web post" describes a process in which an employee transfers company information to a private email address which is subsequently transmitted to a cloud service.

Examination of Work Issued Laptop

An examination of the accused's laptop uncovered the transfer of almost 1600 files onto at least seven (7) USB devices, besides transferring some proprietary information onto his new computer issued by his new employer.

After the FBI reviewed the company's internal computer forensic investigation, it executed a search warrant at the accused's home and uncovered two (2) of the USB drives, and a box containing other proprietary documents.

CASE REVIEW - 2019 - PHARMA TRADE SECRETS THEFT

Just to bring some context to the importance of what the New Jersey pharma security team did in this recent case, I want to draw your attention to another pharma-case post I published in July 2019 titled, Composition of a Chinese Trade Secrets Theft Enterprise: A Family Affair–UPDATE

The 2019 post was an update to a 5-part series I'd written about the theft of trade secrets from another pharmaceutical firm (GlaxoSmithKline (GSK).)

Briefly, in the GSK case, the conspirators' transmitted trade secrets information to their personal email accounts and/or downloaded it onto USB drives too, except, computer monitoring did not uncover the unauthorized transmission of the trade secrets, another employee brought it to GSKs attention after overhearing one conspirator brag about the big money that would come her way.

Here are the two last points I made in that post.

This case reminds us of two fundamental trade secrets protection strategies:

Establish and maintain a vigorous company email monitoring program; and

Conduct periodic background checks of employees who have access to complex and valuable trade secrets.

When you consider the potential impact these two basic IP protection strategies could've had had in disrupting this trade secrets theft enterprise sooner, similar companies–going forward–should zealously implement those actions.

Instead, the thieves were able to disseminate countless trade secrets from 2012 until on or about November 3, 2015.

Terminating this scheme should not have depended on one informant (as important as informant development is) overhearing or being bragged to.

That was an exceptional opportunity (in this case) that companies cannot rely on.

FINAL THOUGHT

Again, in this digital age, it is critical that companies embrace computer monitoring as one (of several) strategies required to keep their intellectual property fenced in.

Ron Alvarez
IP PI Blog
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

---

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.