Objectives

To attain concrete evidence against the alleged accused as; hacking, stealing valuable product license keys, committing piracy, and illegally trading of the reporting organization's products.

Motive

The prima facie motive of the crime, concluded to be 'illegal financial profits'.

Modus Operandi

1. The suspect had hacked into some of the government websites, on which a number software products of the targeted company were being used.
2. He then stole the keys and performed piracy on them.
3. Later, after generating multiple 'pirated license keys' to several products owned by the company, he then sold them to genuine customers online.

Solution

The company needed an expert in eDiscovery and cyber crime investigation, having the indepth know-how of computer forensics.

After facing a number of challenges with other investigating firms, the company approached CCIRC for its expertise in all the demanded disciplines.

The company had specifically chosen CCIRC, because of the company's ability of serving its clients with the following:

1. Foolproof success in resolving the case with a wide range of tools, devices, and techniques.
2. Coming up with new strategies and techniques in each case, particularly planned according to the client's needs.
3. Providing detailed cost figures for each division of the investigation process beforehand, resulting in better management of monetary resources.

Challenges

Challenges laid down by the company in front of CCIRC while presenting the case, were:

1. Extremely tight deadlines.
2. Analysis of a large amount of:
    a. Data, hard drive storages, email accounts, and other devices used to commit the crime.
3. Examination of 100 email accounts belonging to a variety of web mail services.

The Procedure

Documentation

Laptop computer, a number of hard drives, and routers used in the crime were seized from the accused. A complete documentation of the artifacts was made both; before and after performing forensic analysis.

The documentation acted as the proof to verify that no evidence tampering or alteration of artifacts has been performed by the targeted company or CCIRC, during data examination, by any means.

Tools

FTK Imager – The kit was used for creating a forensic image of the seized devices and media for documentation purpose.

MailXaminer – This homegrown, multipurpose email forensics examination tool was used for studying multiple email accounts of the accused from different web mail services.

Specialized Forensic Workstations – These were used to read and analyze the multiple hard drives taken into custody by the investigators.

Strategies

Along with the seized devices and media used for carrying out the crime, there were a number of replicated kits belonging to the company's products in which piracy had been performed with other legal documents that were discovered in the suspect's premises.

Thus, CCIRC took careful measures while obtaining the physical evidences with the classification of investigation stages as:

1. Consultation – The company took a consultation session with CCIRC for the discussion of the case and their needs.

2. Studying The Case – Trails leading to the suspect were discovered with the cooperation of the company and the reporting customer who was allegedly duped in the case.

3. Classification of the Artifacts – A number of digital and document based artifacts discovered from the suspect's premises were classified into categories for an organized investigation.

4. Documentation – Documentation of the evidences taken into custody was done both; before as well as after the investigation to testify no tampering of evidence having taken place.

5. Data Collection & Preservation – Data was later collected from the devices and email accounts of the suspect using advanced forensic software and workstations.

6. Data Recovery – Recovery of deleted evidences was performed using the software along with technical skills and expertise of the case examiners.

7. Verification & Analysis – A thorough verification was done to prove the authentication of the digital evidences and documents collected during the investigation.

8. Presentation – A final report of the entire case details along with the stages of investigation followed out during evidence analysis was generated.

The Law

The case was registered under IPC Section 379 Punishment for theft of the IT Act, 2000.

Results Obtained

The company successfully met their deadlines before time within a valid budget.

1. A large amount of data storing devices, storage media, and most importantly, email accounts were scanned and searched for evidences within a short duration.

2. 17 out of 100 email accounts, with the innumerous amount of emails were scanned with the exact number of email evidences reported.

3. Streamlined analysis was performed on emails consisting of pirated product keys, illegally exchanged with customers.
4. Unmatched precision and organized handling of case related data, evidences, and device, was carried out proficiently.
5. The accused was proven guilty of the charges claimed at him.

Remarks

Remarks by Client: **"***The dedication, efforts taken, and organized conduction of the investigation by CCIRC is highly appreciated. Closure of the case before the requested deadlines within estimated budget came as an extreme surprise to the entire organization.***"**

Remarks by CCIRC: **"***The case involved a number of hurdles but what helped in carrying out an organized investigation throughout was the consistent support and cooperation by the company and complainant.***"**

NOTE: -

If you are a victim of such cyber bullying or want to report a case of cyber bullying, then write us at: - contact@ccirc.in or say hello to us at +91 888 223 3133.