Sûreté du Québec

Operation BASIQUE

Abstract for ILECA - POLCYB Website

Operation BASIQUE was created in July 2006 in response to a desire by Sûreté de Québec (hereafter "SQ") to paint a portrait of computer hacking in Québec. At the time, various isolated events led the SQ to believe hacking activities were on the rise in Québec, notably through the use of Botnets. This discovery marked the start of intensive surveillance of two chat rooms, primarily to identify the individuals frequenting the chat rooms and their status within the group. The follow-up to our investigation was made possible in large part by a partnership with private industry. At the Microsoft Law Enforcement Tech Conference in Redmond, Washington (U.S.) in October 2006, we were able to appreciate the many resources and services Microsoft offers to law enforcement organizations. Microsoft provided a tool to help the botnet investigations. The community also helped in the investigation by means of information provided and complaints lodged by citizens, businesses, and government organizations.

With suspects having been identified and offences having been committed, a sweep was therefore the next logical step to substantiate evidence gathered to date and confirm the identity of suspects retained for the investigation. On February 20th, 2008, over 150 SQ police officers, in partnership with a dozen RCMP officers, were called upon to search 17 areas and arrest 17 suspects aged 17 to 26, including four who were minors at the time the offences were committed. The searches led to the seizure of 54 computers, 20 external hard drives, 11 USB flash drives, 1,227 CDs and DVDs, 117 diskettes, and a number of other peripheral devices, such as MP3 players, digital cameras, cell phones, etc. Among the suspects, eight were served an arrest warrant for the following charges: illegally obtaining computer services, hacking computer data, and possession of passwords for the purpose of committing these offences. The maximum sentence is 10 years. The suspects were then released under conditions imposed by the court. Disclosure of evidence obtained following the investigation and analyses is set for fall 2008.

Analysis of the material seized up to now (about 50%) has helped substantiate the evidence gathered during the intelligence phase at the time of the criminal investigation per se. It also made it possible to identify a number of collateral crimes using botnets and brings the scope of the investigation as follows:

- 100 botnets involved,
- Over a million different masks used by IRC robots,
- Over 500,000 different IP addresses from over 114 countries, including primarily, ranked in order: Poland, Brazil, Mexico, Argentina, Chile, Italy, Germany, the United States, Canada, and Russia.
- 150$ million US in direct and indirect damages,
- The crimes committed targeted not only individuals connected to the Internet, but also a number of private and public companies, thereby compromising the confidentiality of the personal information of all their clients. These crimes included the following:

    - Ø Interception of private communications by means of : sniffing data traffic, keylogging, obtaining usernames and passwords for various online resources
    - Ø Bank phishing
    - Ø Denial-of-service attacks
    - Ø Click fraud
    - Ø Warez hosting

The consequences of these collateral crimes are serious, especially in the case of interception of private communications. It results in total identity theft, which may have two distinct types of repercussions on its victims. The first is direct financial loss for both the consumer and the merchant. The second type of repercussion involves indirect costs that victims must assume, namely a tainted reputation and a bad credit rating, which may follow the victims for a very long period of time. Operation BASIQUE enabled us to uncover a vast network of identity thieves, understand the techniques they use, and prevent possible repercussions, all through the seizure of their computer equipment.

Project BASIQUE is a perfect example of complementarity among criminal intelligence, investigation, and computer forensics. It demonstrates the SQ's leadership and ability to stop and bring to trial criminals who commit serious Web-related offences. The project also demonstrates the success obtained when a hacking investigation is initiated, because in investigations based on accusations, more often than not suspects remain practically unidentifiable. Lastly, the project underscored the importance and need to work in partnership with both other public bodies such as the RCMP, and privates companies such as Microsoft. Media coverage of this police operation was extraordinary and demonstrated how important cybercrime is to the public. Since the arrest of 17 hackers was announced, the effects on the community have been felt. Accusations are up, as is people's interest in protecting their computer systems and personal information. A number of awareness campaigns in this regard are being developed in Québec to optimize the prevention of such incidents. The message to hackers is clear: computer crimes will not be tolerated and law enforcement agencies are in a position to fight them.