Stopping Cyber Criminals in Their Tracks

Accelerating Your Mission.

Of the many daunting challenges faced by law enforcement in investigating cyber crime, probably the most difficult is locating and actually putting handcuffs on cyber perpetrators. Sûreté du Québec, the police force of the Canadian province of Quebec, needed a more effective way to map and connect the dots of a complex criminal computer network, in what would prove to be the country's largest-ever police operation conducted against hackers. The sophisticated entity resolution, data extraction and complex analysis capabilities of i2's *Cyber* solution enabled investigators to navigate a maze of participants and transactions, map the network, and connect illegal actions to the cyber criminals, leading to their arrest.

"Before mapping in Cyber, I had difficulty understanding the interactions in thousands of spreadsheet lines."

– Inspector François Blanchard, Sûreté du Québec

Situation

In 2008, Sûreté du Québec, the police force of the Canadian province of Quebec, embarked on Operation "Basique"; at the time, this was the largest police operation ever conducted in Canada against cyber crime. Their target: computer hackers who had developed a network that controlled 100,000 personal and company computers in 75 countries.

Because of the surreptitious nature of cyber attacks, and the many layers and byzantine structures of a hacker network, in many cases it can be next to impossible to track the originators of online crime. The suspected hacker ring used malware known as *worms* to infect the proxy computers used in their network. Once infected, these computers were assembled into a sleeper network known as a BotNet, which could be commanded to launch virtual attacks against various Internet sites.

BotNets are rapidly rotating networks of hijacked computers that criminals use as proxies to commit their attacks and mask their identities. As a BotNet grows, the origin and participants in the attacks become more geographically dispersed and the networks more complex and less centralized. BotNets can even infect small applications that can be inserted into social network sites such as Facebook and LinkedIn.

The veil of the Internet serves as a complex layer of insulation and disguise between cyber criminals, their victims, and the law enforcement authorities attempting to investigate and prevent their illegal activities. Sûreté du Québec was using a common spreadsheet software, which assembled huge, cumbersome tables that required extensive manual cross-referencing. The police force needed a more effective way to cut through the complex maze of participants and map the network to the players and their transactions.

Overview

Location: Quebec, Canada

Industry: Law Enforcement

Customer: Sûreté du Québec, the police force of Quebec

Challenge: Cyber Crime

i2 Products Used
Cyber, Analyst's Notebook

Solution

i2 introduced Sûreté du Québec to the *Cyber* toolkit, which is an advanced analysis solution providing deep levels of connectivity, activity and temporal mapping. (Since 2002, Sûreté du Québec has also used *i2*'s *iBase*, which captures and manages data and shares actionable intelligence that supports intelligence-led operations.)

Analyst's Notebook, a key element of the *Cyber* solution set, was used to map the network. Several layers of investigation were undertaken, which included analyzing multiple data sets and tracing complex relationships and transactions:

- Identifying the hacking tools ("worms") being employed to infect computers and create the BotNet ring of slave computers
- Tracing the route of the worm the hackers used to infect the computers they wanted to control and finding which computers it had infected
- Identifying the Internet Protocol (IP) address of the infected machines and defining the Uniform Resource Locator (URL) vectors of infection
- Establishing the relationships of the slave machines that were unknowing participants in the peer-to-peer network and connecting these infected computers to the larger BotNet, being controlled by the hackers
- Defining the "Command & Control" (C&C) machines that were giving the orders, which eventually led to the connection of the machine addresses belonging to the cyber criminals behind the hacker ring

Through *Cyber's* powerful mapping capabilities, the police were able to connect the illegal actions to the perpetrators. A key break in the case came when "the arrestee and the other accused were present in the same chat room and took the opportunity to discuss their achievements and exchange tips," said the prosecutor in the case. The perpetrator even went so far as to try to package and sell his methodology for committing the fraud.

Outcome

The Sûreté du Québec estimated that the Internet pirates had caused damage totaling tens of millions of dollars, taking into account the cost of repair or replacement of computers for the affected victims. Among these were hotels in Quebec province and government institutions in Quebec and elsewhere in Canada that have not been publicly identified. The cost to the victims could have been significantly higher as the hacker ring and their BotNet grew, had they not been stopped when they were.

About i2

i2 is the leading provider of intelligence and investigation solutions for defense, national security, law enforcement and commercial security. More then 4500 organizations in over 150 countries rely on the i2 Intelligence-Led Operations Platform to proactively deter, prevent, predict and disrupt the world's most sophisticated criminal and terrorist threats. i2 started the intelligence revolution in 1990 and continues to lead the industry in innovation with products like *Analyst's Notebook*® and COPLINK®. These solutions help public safety officers, analysts, managers, detectives and investigators uncover hidden connections faster, enabling collaboration and delivering critical information to the point of need.

For more information, please visit
www.i2group.com

Accelerating Your Mission.