Palantir

IMPACT STUDY

UNCOVERING GHOSTNET

Between June 2008 and March 2009, a team of Canadian investigators used Palantir to reveal a network of over 1,200 infected computers in 103 different countries. This network, which they called "GhostNet," included "high value targets" such as the Indonesia Ministry of Foreign Affairs, the Indian Embassy in Kuwait, and the private computer of the Dalai Lama.

THE PROBLEM

Investigating cyber crimes can be an overwhelmingly complex task. Unlike traditional investigations, where detectives piece together evidence to solve a crime, the main challenge of cyber investigations involves figuring out how to handle the enormous data scale. For this reason, in the early stages of the GhostNet investigation, the researchers spent most of their time combing through troves of electronic data sources to determine which information sources were useful and which were not. What they really needed was a software platform that could bring all their data sources into one environment, where they could distinguish the useful information from the digital noise.

PALANTIR'S SOLUTION

The investigation was a joint initiative between the SecDev Group and Citizen Lab, two information security organizations based in Canada. It did not take long for the investigators to recognize that traditional, automated methods of cyber detection were inadequate to the task of exposing this advanced persistent threat; computer algorithms alone could not uncover such an intelligent and adaptive adversary. So they turned to Palantir, which applies the best of human and computer approaches to investigating cyber crime.

After installing the Palantir Platform in less than two weeks, the researchers integrated several large datasets into Palantir, including network monitoring data, interview data, and forensic technical data. With this information in Palantir, they used the Graph application to map out the compromised networks and possible perpetrators. They also used the Map application to trace the attacks to their original locations. After testing and confirming numerous hypotheses, they submitted a comprehensive report to the appropriate authorities in March 2009.

PALANTIR'S IMPACT & RESULTS

» The investigators discovered **over 1,200 infected computers** in **103 different countries**.

» Almost 30% of these computers were considered high value, including the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan.

» "This is believed to be **the first time** researchers have been able to expose the workings of a computer system used in an intrusion of this magnitude."

– The New York Times, March 28, 2009

FOR MORE INFORMATION

www.palantir.com