Max Chi
chi19
hw#13
4/24/3018

GhostNet

In a 10-month investigation from 2008-2009, the Information Warfare Monitor (IWM) conducted an extensive research investigation that uncovered thousand machines in the Office of His Holiness the Dalai Lama (OHHDL) and other Tibetan organizations had been infected with malware. In the process of searching for those responsible for the infectious malware, they discovered the existence of a deep malware net known as GhostNet who had control over a number of control and command servers.

The investigators used WireShark allowed the collection of packet data from multiple computers in locations such as OHHDL, Offices of Tibet in New York, Tibetan Government in Exile, and more. The Palantir Cyber was also used to uncover the locations and links across multiple computers that were affecting the network. Analysis of this data showed that the malware utilized http requests and uploaded the private information to CGI scripts which were hosted through bypass websites. Even more servers were uncovered by tracing the links between control servers and command servers.

In order to lure the attackers, the investigators used a honeypot computer, which would voluntarily become infected, to lure the attackers and proved fruitful in that it discovered the IP addresses of four specific control servers. Using an IP lookup on the IP addresses unveiled a gh0st RAT that utilized commercial Internet accounts located on Hainan, an island belonging to People’s Republic of China.

It was later uncovered that locations of the control servers resided in Hainan, Guangdong, and Sichuan in China and that the fourth control server was located at a web-hosting company based in the United States. The command servers were found to be located in Hainan, Guangdong, SIchuan, Jiangsu and Hong Kong.

The GhostNet Trojan worked by creating web pages that contained “drive by” exploit code which would infect any computer that accessed the page. The attacker(s) also engaged in spear phishing, where relevant emails containing PDFs and DOCs were sent to which upon execution would create back doors that triggered a connection from the infected computer to control servers. The attackers could then issue commands to ranging from screen captures to operating webcam, basically having complete access to the infected computer, giving the attackers total control.

Shadows In The Cloud

Following the discovery of GhostNet in 2009, researchers at the Information Warfare Monitor (IWM) discovered cyber-espionage operation that had stolen classified documents and emails from the OHHDL, the Indian government, and numerous other high-level government networks. The investigators traced its steps back to the similar approach to unveiling GhostNet as well as other techniques such as DNS sinkholes setup in domains that were previously susceptible to the aforementioned attacks.

The discovery of GhostNet had shown that numerous amounts of Tibetan and Indian computers had been compromised linking to computers of Indian embassies in various locations like Serbia, Italy, the UK, and many more. Once again, the investigators conducted extensive field work based on the Action Research Literature which had been evolving since the 1940s, feeds into the fusion methodology that guides our overall investigatory process by employing with ethical and participatory observations in combination with grounded research with technical interrogation, including network monitoring activities.

It was revealed through extensive investigation that the computer on TennorNet that was generating malicious traffic belonged to a Mr. Serta Tsultrim, a Member of the Tibetan Parliament, editor of the Tibet Express as well as the director of the Khawa Karpo Tibet Culture Centre. The investigators utilized numerous data gathering and analysis techniques like DNS Sinkholding, Malware Analysis, Command and Control Center Topography, Victim Identification, Data Recovery for data analysis, and Palantir and WireShark for data collection.

The investigators found that the attackers had created 5 Yahoo! Mail accounts as a component of command and control, where when a computer was infected, the malware would create folders in the accounts inbox folder that included the computer’s name, operating system, and IP address. An email would be sent to the account which contained a command with additional malware as an attachment, and the next time an infected computer logs into the email account the malware would be downloaded.

Through thorough investigation, it was discovered that there were 27 different forms of malware on the command servers which all had the destructive potential, including but not limited to screen capturing, remote shell, keylogger and more. This ultimately allowed the attacker complete control of the compromised computers.