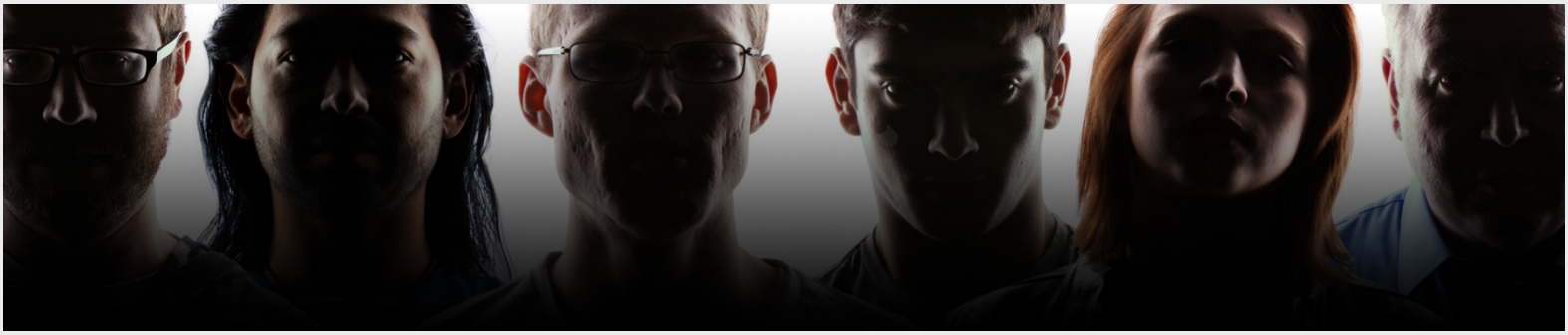
SPEARTIP®

CYBER COUNTERINTELLIGENCE

Outmaneuver Your Adversary™



INVESTMENT FRAUD

The Growing Threat to Your Financial Security

Financial firms must be proactive and vigilant for attacks focused on their customer's data and financial interests.

Kris Bleich, CISSP, EnCE, C|EH

As legal standards and regulations evolve, institutions must continue to be proactive as it relates to data security. Both internal and external threats pose a significant risk to an organization's high value data. Financial firms must be proactive and vigilant for attacks focused on their customer's data and financial interests.

Banks and financial institutions continue to be popular targets for attackers. In October, 2012, PNC Financial Services was the victim of a prolonged attack. PNC Financial Services CEO James Rohr, in a CNBC interview, stated that the targeted attack "just pummeled us".

Attacks on financial institutions have evolved and attackers interested in compromising financial accounts are targeting individual investor accounts as a way to gain access to the client's account information. In 2012, The Financial Industry Regulatory Authority (FINRA) issued an alert citing these attacks. The FINRA alert noted that the Federal Bureau of Investigation, along with several other agencies, have also issued fraud alerts citing an upward trend in these types of attacks.

The FINRA alert described attacks in which attackers compromised the email accounts of individual internet users. After gaining access to these email accounts, attackers contacted the brokerage firm requesting a funds transfer to a third-party account, which is often an overseas account. In some cases, the attackers spin a tail of urgency, stating that they will sign the authorization letter for the transfer later. In other cases, the attackers obtained a previous check or other document containing the victim's signature from the brokerage firm or victim's email inbox.

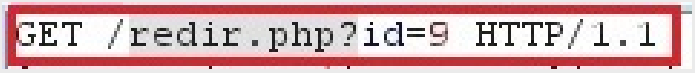
In December, 2011, SpearTip received a phone call from an Investment Firm indicating that the firm had been the target of just such an attack. Two wire transfers totaling approximately $90,000.00 had been made to an overseas account in Australia at the apparent request of the client. Forensic images of the systems at the Investment Firm were obtained. In addition, forensic images of the personal laptop of the client were obtained.

Emails, which appeared to be from the client, were received by the Investment Firm requesting an urgent transfer to a third-party overseas account. The emails stated that an emergency had developed and that the client was unavailable by telephone. Attempts by the Investment Firm to contact the client by phone failed. The following details the investigation and conclusions for this case.

The forensic analysis began by examining the emails that appeared to have been sent by the client to the Investment Firm. The originating IP address for the email requesting the transfer of the funds was located in the header of the email.

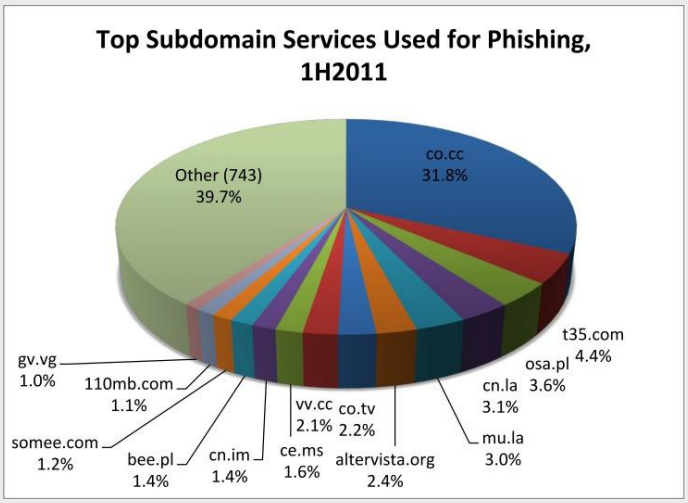
This IP address was traced back to the country of Malaysia.

An analysis of the client's laptop located the malicious .htm file, 9[1].htm, within a temporary directory for Internet Explorer. This file was created on December 3, 2011 and contained a link to a php script, "http://ftsoki.co.cc/redir.php?id=9". Further analysis of this .htm file found that this malicious script would be downloaded onto a user's system after visiting a compromised website.



An analysis of the internet history of the client's laptop located the website likely responsible for the introduction of malware onto the client's laptop.

Further research was conducted into the web address "http://ftsoki.co.cc". These domain addresses are free addresses offered by a Korean company. ".cc" is the Internet Country Code Top Level Domain for the Cocos (Keeling) Islands, which is an Australian territory in the Indian Ocean. The "co.cc" domain, as a whole, has been identified as a common source of email spamming and phishing attacks. The Anti-Phishing Working Group (APWG) identified the "co.cc" domain as a prominent threat to users, accounting for 31.8% of all phishing attacks. As a result, in July 2011, Google removed 18 million web addresses from the "co.cc" domain from its search index, preventing any web addresses from this domain from being displayed as a result of a user search on Google.com.



The totality of SpearTip's forensic analysis identified a pattern of compromise beginning in Malaysia. SpearTip interviews at the Investment Firm obtained information identifying a sequence of events leading up to the transfer of approximately $90,000.00 to a third-party account in Australia. Malware was located on the client's laptop which identified a point of compromise for login credentials on the system. A detailed analysis of the malware on the system identified a web address in the Cocos Islands, which was the origin for malicious applications that likely compromised the client's login credentials.

In addition to securing the corporate environment, Investment Firms must take proactive steps to educate its employees and defend against attacks launched by individuals posing as a trusted authorized agent. While a company can exercise control over systems within its network environment, client systems that are not adequately protected present a risk to client data at Investment Firms. Companies must maintain and adhere to strict protocols regarding the transfer of funds. Typically, a signed authorization form is required; however, this protection may be ineffective if an attacker gains access to the client's scanned signature after compromising the client's email account. In the event that an attack on the company is detected, actions should be taken to identify the origin and scope of the compromise, including forensic analysis of company and client systems. A swift response and subsequent forensic analysis is critical to defend the company against subsequent legal claims from the client.