

THE PROFESSIONAL CRIMINAL



THE ROMANIAN PHISHING EXPEDITION

In one of the most celebrated cyber counterintelligence operations in history, SpearTip operatives provided the FBI and Interpol with detailed information leading to the arrest and conviction of key figures in an organized Romanian cyber crime syndicate.

The case began when a \$20 billion global giant discovered signs that one of their servers responsible for credit card payments may have been compromised. Following protocol, company officials contacted a Payment Card Industry (PCI) audit firm to determine if credit card data had been stolen. The company also contacted SpearTip operatives to conduct a full analysis of all systems and networks.

While the PCI audit proved no credit card data had been breached, findings from the SpearTip team revealed a significant intrusion that was actually using the company's servers for criminal activity unbeknownst to anyone within the organization.

Using a cleverly devised plan and malware that embedded itself invisibly within the company's systems, Romanian criminals were using customer e-mail addresses in an elaborate phishing scheme. The criminals sent innocent consumers e-mails, disguised as security notices from eBay and PayPal, to obtain

personal and financial information. The e-mails were launched using malware-infected company servers, that also relayed information-filled replies back to the crime family in Romania. It was the perfect crime. Almost.

SpearTip operatives found bits of unusual and uncharacteristic data throughout the company's systems during our investigation. We then analyzed the data from a variety of different disciplines, while also searching for associated information in areas of the Internet often frequented by criminals.

Following trace evidence created during the phishing scheme, SpearTip identified not only the source of the crime, but obtained the names and photos of the criminals who masterminded the entire plan.

With information in-hand, company officials and representatives from SpearTip turned over full criminal reports to the FBI and Interpol. Shortly thereafter, international policing authorities arrested members of the Romanian crime syndicate, who are today serving long sentences in jail.

(As a matter of privacy and confidentiality, SpearTip never names clients when providing case studies.)