

## Cloudmark Research Report

### New phishing attack spotted that utilizes VoIP technology

Date: April 21, 2006  
 Author: Jason Harbert

The Cloudmark Collaborative Security Network (CCSN) recently spotted a new variant of the classic e-mail phishing scam inside of our network. The attack circulates via e-mail from a bank and requests that customers call an "official" number to verify account information. The phone number connects the customer over voice over IP (VoIP) to a PBX system that utilizes an interactive voice recognition (IVR) application. The customer then provides his personal account information, which, in turn, is transcribed and saved by the IVR system.

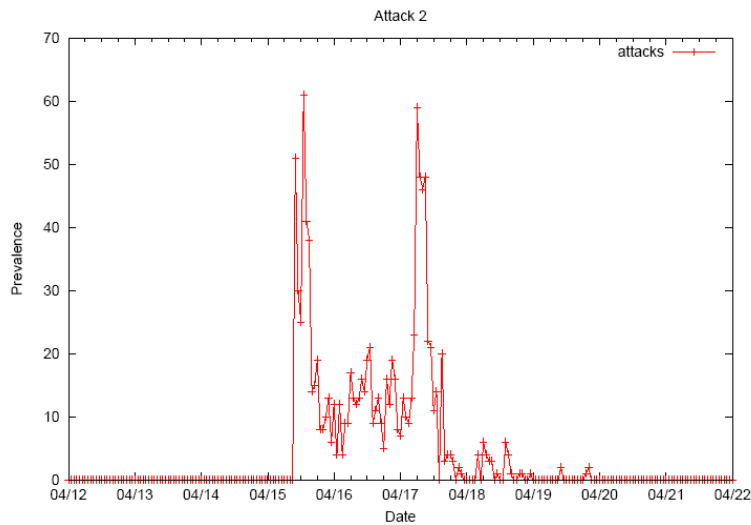
#### Analysis:

Cloudmark recognized and blocked the new attacks early on, via one of our specific fingerprinting algorithms that is specifically designed to detect unique features of attacks - in this case, phone numbers. After discovering the new attack variant, we performed an analysis of phishing attacks that contained phone numbers on our system. As a result, we identified other variants of the same attack.

We subsequently performed analysis into the scope and timeframe of the attack. Two attack timelines are shown in Figures 1 and 2. Both show an initial heavy prevalence of attacks, which begin to lighten in the following days until they are not seen at all.



*Figure 1. The timeline of this attack shows high points during daylight hours, but the attack as a whole tapers off over a six day period.*



*Figure 2. The timeline of this attack shows two moments of heavy attacks, followed by a sharp drop-off until the attack disappears.*

### **Conclusion:**

While the impact of the VoIP phishing attacks on our user base was negligible, the method and diversity of the attacks make them unique among phishing scams. Though the cost associated with running a phishing scam involving phone systems remains higher than classic website-based phishing scams, the costs associated with setting up a VoIP system continues to drop and new phone-based attacks may continue to rise. Furthermore, with no link to a phishing website in the email, fraud detection software may not be able to identify and block these scam email messages. However, our fingerprint-based, collaborative security network has shown to be effective at blocking new attacks, regardless of the type or method of the attack, without a supervised learning process.