A New Twist in Account Takeover

FBI Warns of Scam Linked to E-mail Compromises

A so-called "man-in-the-e-mail" scam that's targeted at least three Seattle-area businesses reflects a growing trend in account takeover compromises.

Fraudsters intercepted legitimate e-mails between the businesses and their suppliers and then spoofed subsequent e-mails impersonating each company to the other, according to a Dec. 2 warning issued by the Federal Bureau of Investigation. Losses linked to the attacks have so far totaled approximately $1.65 million.

The affected businesses were fooled into thinking they were sending money to an established supply partner in China. But the money was actually being sent directly to bank accounts managed by the attackers, and not from the supplier who originally made true contact, according to the FBI.

John LaCour of the online security firm Phish Labs says these types of e-mail attacks are becoming increasingly common. "We have seen a huge increase in the amount of Webmail accounts targeted by phishers in the last year," he says. "By compromising the e-mail accounts of buyers and sellers using these marketplaces, fraudsters are able to spoof the e-mails between buyers and sellers necessary to redirect shipments and payments."

Source of Attacks

Most man-in-the-e-mail attacks originate from China, LaCour says. And many of the sites attackers use to launch their spoofed campaigns have been nearly impossible to shut down, he says.

"These phishing sites are some of the longest living ones out there".

"We know of some that have been live for over two years".

The sites survive because the spoofed e-mails they are sending out aren't detected by current anti-spam and phishing methods, he says.

"They either spoof many brands at once - such as four or more Webmail providers - or are generic enough not to draw attention from any company that might pursue shutdown of the phishing site," La Cour says.

Tips from the FBI

The FBI is warning businesses as well as consumers to be wary of e-mails from unrecognized sources and take steps to double-check the source of origin. In some cases, the metadata on the spoofed e-mails in the Seattle-area incidents indicated that they actually originated in Nigeria or South Africa, the FBI notes.

Among the FBI's other top recommendations for avoiding falling victim to such schemes:

- Use out-of-band verification, such as telephone calls, and second-factor authentication that does not rely on e-mail, for all monetary transactions;
- Avoid free Web-based e-mail accounts, such as G-mail and Hotmail;
- Use digital signatures;
- Always forward business e-mails, rather than simply replying, to ensure e-mails are going to a legitimate address that is manually entered;
- Never open spam; delete it immediately;
- Beware of odd changes in business practices, such as a supplier suddenly asking that you contact a sales representative through her personal e-mail address.
- If you see any unusual behavior, at least contact your supplier.
- Protect your personal information all the time, including webpages you browse.