eRiskHub®

Email Hacking, Spoofing and Phishing for Stolen Cash

Cases

- Ubiquiti Networks Inc. disclosed that cyber thieves stole $46.7 million using an increasingly common scam in which bad guys spoof email communications from executives at the victimized businesses in a bid to initiate unauthorized international wire transfers, to steal money.
- Con artists made off with a whopping $17.2 million from one of Omaha, Nebraska's oldest companies, the employee-owned commodities trader The Scoular Co. According to Omaha.com, an executive with the 800-employee company was duped and wired the money in installments to a bank in China after receiving emails ordering him to do so.

How Does This Happen?

❶ **Method 1: Corporate Email Account Is Hacked and Used to Dupe Others:**

According to an alert from the FBI, cyber thieves stole nearly $215 million (see chart below) from businesses in 14 months using a scam that starts when business executives or employees have their email accounts hijacked. The so-called CEO phishing fraud starts with the email account compromise for high-level business executives (CEO, CFO,). Posing as the executive, the fraudster sends a request for a wire transfer from the compromised account to a second employee within the company who is normally responsible for processing these requests (for instance, accounts payable or the comptroller).

Experts warn that these requests for wire transfers are typically well-worded and specific to the business being victimized, and do not overtly raise suspicions to the legitimacy of the request," The fraudster often knows that the CEO/CFO is not in the office on that given day (this from prior reconnaissance such as calling the company and asking for the CEO or CFO to find out their schedule).

The BEC is a global scam with subjects and victims in many countries The IC3 has received BEC complaint data from victims in every U.S. state and 45 counties. From 10/01/2013[1] to 12/01/2014, the following statistics are reported:

- Total U.S. victims: 1198
- Total U.S. dollar loss: $179,755,367.08
- Total non-U.S. victims: 928
- Total non-U.S. dollar loss: $35,217,136.22
- Combined victims: 2126
- Combined dollar loss: $214,972,503.30

The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase.

(Source of graphic: KrebsonSecurity.com & IC3.Gov)

❷ **Method 2: Spoofing the CEO's Email and Then Phishing the Comptroller:**

In this approach the fraudster sends an email that appears to be from the CEO (let's say, for instance, John.Smith@Acme.com). At a closer inspection of the sender's email address header details one might note a phony domain is being used to masquerade as the alleged CEO sender (the email is actually coming from the fraudster at John.Smith@Acme1.com or some similar variation). Knowing that most people are too busy to notice, the fraudster exploits human weakness to obtain critical information.

How Can These Scams Be Prevented?

There are a number of options for mitigating cyber theft through phishing, hacking and spoofing:

- Adopt two-step or two-factor authentication for email, where available, and/or establish other communication channels such as mandatory telephone calls to verify significant transactions.
- Exercise restraint when publishing or posting about employee activities on websites or social media accounts, to limit access to the type of information that makes fraudulent missives more convincing.
- Secure messaging by deploying a signed and encrypted email solution.
    - Note that this is not a solution in the case of the attacker who has hijacked the CEO's legitimate email account.

Finally, note that spam filters typically will not work or flag the spoofed email because they are targeted phishing scams and not mass email.

---

eRiskHub®, powered by NetDiligence®

NetDiligence® is a cyber risk assessment and data breach services company. Since 2001, NetDiligence has conducted thousands of enterprise-level cyber risk assessments for organizations of all types and sizes. NetDiligence services are used by leading cyber liability insurers in the U.S. and U.K. to support both loss-control and education objectives. NetDiligence hosts a semiannual Cyber Liability Conference attended by risk managers, privacy attorneys and cyber liability insurance leaders from around the world. NetDiligence is also an acknowledged leader in data and privacy breach prevention and recovery. Its eRiskHub® portal (www.eriskhub.com) is licensed by cyber liability insurers to provide education and breach recovery services to their policyholders.