BANK INFO SECURITY®

When You Can't Even Trust Anonymous

Trying to Make Sense of False Claims of a Cyberattack

By Eric Chabrow, *September 26, 2012.*

You just don't know who to trust these days, especially when they're anonymous or Anonymous.

In the past month, an individual claiming to be from AntiSec, a group affiliated with the hacktivist collective Anonymous, took credit for hacking an FBI agent's laptop computer and pilfering millions of identifications of Apple devices. As it turned out, the hack was against a private company and not the feds [see ***Alleged FBI Hack: Much Ado about Nothing***].

> ***With so much hype and confusion around cybersecurity, falsely claiming an attack can have some effect.***

When websites of an untold number of small businesses operated by provider GoDaddy went offline earlier this month, a tweet from an individual claiming to be an Anonymous member took credit for the disruption, while a second tweet from another Anonymous claimant said the anonymous collective wasn't behind what was described as a distributed denial of service attack [see ***Did Anonymous Target GoDaddy?***]. In truth, GoDaddy says internal database problems caused the website interruptions.

And, although not a digital theft, someone has claimed to have stolen Republican presidential nominee Mitt Romney's tax returns, and the unknown claimant is demanding a ransom of $1 million to prevent the documents from being sent to news organizations on Sept. 28. The accounting firm where the Romney tax records are said to be stored denies anyone broke into its office.

Such claims cloud the environment where security practitioners work. Of course, not every claim is false. A number of attacks claimed by so-called hacktivists have proven to be true, as they post on the Internet data stolen from sites to verify their claims.

Much Hype and Confusion

Yet, these assertions themselves - especially before they're verified - can have an impact on the security of governments and businesses. "In the current era, with so much hype and confusion around cybersecurity, falsely claiming an attack can have some effect," says Jim Harper, director of information policy studies at the think tank Cato Institute. "But it's unlikely to work for long because organizations will learn how to communicate about fake attacks and the press and public will become more savvy."

Harper says individuals making false claims play what he calls the information game. "Along with trying to affect what has actually happened, organizations and their challengers are both vying for control of what people think has happened," Harper says. "It's often to the attacker's benefit to keep the fact of the attack unknown to the organization. You'll see this in crime or espionage. At other times, the attacker plays the information game off of a third party, the public, because the public can affect the organization as much or more than the attacker can alone."

Is too much attention paid to hacktivists' claims - whether true or not - diverting attention from other types of threats?

"A threat is a threat is a threat, whether motivated by hacktivism or anything else," says Tom Patterson, lead cybersecurity consulting partner at CSC, an IT services company. "While sharing information about real threat information is generally useful, early reporting on false claims tends to cause more harm that good."

The Blame Game

Yet, as the GoDaddy incident demonstrates, blaming disruptions on security failures can distract attention from other problems that plague technology and have nothing to do with security.

"The perception that all disruptions come from attacks is the effect of two years of major **breaches** and successful attacks starting with the Sony PlayStation Network [see ***Sony Breach Ignites Phishing Fears***] and including the successful breach of RSA [see ***RSA Says Hackers Take Aim At Its SecurID Products***]," says Surviving Cyberwar author Richard Stiennon. "It is not a disservice to IT security organizations; it is derived from the true insecure state of most organizations."

Still, that insecurity makes reporting on these hacking claims difficult. In the incidents involving the GoDaddy disruption and FBI hack, the "facts" were laid out, including the FBI's denial its agent's computer was breached, leaving it to you - the reader - to be the final arbiter of the truth. For journalists, that's a copout. We should do a better job determining the truth. But it's not that simple when hacktivists' claims often prove to be true. It's tough to ignore such stories, so the

news consumer must approach them skeptically, especially when the source remains anonymous or Anonymous.