BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

October 2015 | Briefing 10

CYBER CRIMINALS ARE TARGETING YOU.

AND YOUR TRUST CIRCLE.

As your enterprise's reputation grows and becomes more and more trusted, third parties are more and more likely to use your corporate brand and logo, to attack your clients, your employees and the general public. But in a rapidly growing number of attacks, the cyber criminals will hijack names, photographs and even create fake online profiles of key company leaders, including executives, board members, and their families, to lend credibility to their cyberattacks.

The classic cybercrime gambits – phishing attacks, domain theft, and social domain fraud are usually perpetrated using only logos, corporate design standards, and carefully chosen social domain names. But these attacks are even more effective when they use an executive name or image. And **as high-profile social media activity becomes a larger and larger component of a PR or outreach plan, an enterprise's risk of compromise increases**.

Spoofed emails are nothing new – simple brand-based phishing is one of the most common of all cyberattacks. But spoofed emails that seem to originate from key executives are another matter altogether. These kinds of attacks are essentially social engineering assaults. During the planning/early phase of the attack, the cybercriminals mine online information to identify key leaders and key employees at the targeted firm, building out lists of responsibilities, chains of command, and contact information. Then, **when the thieves are ready to strike, they masquerade as company executives, sending appropriate communications that appear to be directly from the executives,** making plausible requests to employees through seemingly trusted channels.

HELP WANTED?

BrandProtect recently thwarted a cybercrime scheme based on counterfeit job postings – these postings included a seemingly legitimate email to a key executive at the company. A quick LinkedIn check would confirm that the key executive worked for the company, giving the email address seeming legitimacy, but the email was not to a company domain, it was to a domain controlled by the bad guys. People responding to these job postings were sharing their information with the criminals.

Senior Vice President, Asset Management
Keller Augusta Partners, Cranston, RI
Proven executive leadership skills. The firm is seeking a Senio

Vice President, Associate General Counsel
IMG College, Cranston, RI
Excellent interpersonal and communication skills which will en personalities and styles in a fast-paced business...

Regional Vice President of Partner Management
GoNoodle, Cranston, RI

$46 MILLION, GONE IN SECONDS

In one recent example, networking firm Ubiquiti Networks Inc. **reported a loss of $46.7 million from seemingly legitimate executive requests to members of the company's finance team for wire transfers of funds** from the corporate to third party accounts! The requests seemed to originate from company executives and the duped employees thought they were complying with instructions for the very top of their company.

IN 2014, OVER $200 MILLION WAS STOLEN FROM US CORPORATIONS VIA EXECUTIVE IMPERSONATION SCHEMES.

(THE FBI)

This attack didn't happen overnight. **The criminals harvested lots of information about the inner workings of the company by mining online sources, including tracking social media profiles, online activities and company news.** As they built up their nefarious dossier on the company, they gained confidence that they could assume the needed corporate identities and spring their trap.

LINKEDIN... BUT TO WHO???

We've all Googled ourselves, but have you looked past the number of hits you received and inspected the information that is available about you publicly? **It is astonishing, the amount of personal data that is readily available you online.** This information is not just available to the good guys, the bad guys have access to it, too. And there is a lot of additional information available, real estate transactions, for example, if you know where to look. And the bad guys know.

It's the same for online profiles and friends lists. Many professionals keep an online profile at one or more professional networking sites like LinkedIn. But **these profiles can be copied and inserted into new counterfeit profiles**, which are used to collect friends, and build trusted circles. Finally, there is a wealth of additional information available for the investment of just few dollars – addresses, dates of birth, etc… With all this information at their fingertips, it's no wonder that a cybercriminal can assume an identity quickly and convincingly.

You are Vulnerable to Attack... And You May Be Being Used To Attack Others

One of the most troubling aspects of this kind of masquerading attack, is that lots of damage can be done to you, your reputation and your enterprise reputation without the attack ever crossing, or even touching your traditional security perimeter. **The criminal operates beyond your perimeter, collecting information about you and your firm that is public or easily accessed, and then using that information to prey on others** who are also outside the perimeter. Customers, partners, competitors, employees and prospective employees can be led to believe they are working with you, when in fact they are communicating with a cybercriminal.

Executive Masquerading is just one of the ways cyber criminals can attack your company and you. CISOs need to take action – starting today – secure your executives and your company reputation beyond the perimeter.

TAKE CONTROL – INITIATE SECURITY TEAM MONITORING FOR POTENTIAL EXECUTIVE AND EMPLOYEE MASQUERADING

LinkedIn

Kendra Jennings
Chief Operating Officer
XYZ Corporation
2010-present

It sounds simple, but this is an arena where an ounce of prevention goes a long way. **A simple online search of key executives will be eye-opening to you and your security department**. A more complete executive audit, usually conducted by a firm specializing in online threat detection, analysis, and mitigation, can provide you and your security team with valuable insights about the depth and breadth if information available online. After that spot check, **it usually makes sense to implement consistent preventative cyber-monitoring for online activity that is made using your and your executive team's names**. In some cases, companies implement cyber monitoring for the executive team, board members, and the spouses of the executive team and board members.

Don't take a chance – you can begin reducing your risk of masquerading attacks today. Assess your current exposure through a simple audit. Back up your good first steps with consistent cyber monitoring of executive mentions and activity. Whenever your executive names appear online, make sure that you know the context of the mention. If you can't explain the appearance, dig deeper, you may be looking at the beginnings of a social engineering scheme.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect, helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.