Duplicate Executive Social Media Accounts Put F500 Enterprises in Peril

BrandProtect Analysis Detect Potential Social Media Masquerades

TORONTO, ON. – Nov. 15, 2016 – New research by BrandProtect, a leader in Internet threat detection, analysis and mitigation, has uncovered numerous duplicative Twitter and LinkedIn accounts among Fortune 500 leaders, raising concerns about potential security vulnerabilities.

Analysts at BrandProtect reviewed profiles for the 54 CEOs at Fortune 500 companies using Twitter and the 187 CEOs using LinkedIn. Of these CEOs, 19 percent were represented online by multiple Twitter accounts, while 9 percent had multiple LinkedIn accounts.

"Even carefully managed Fortune 500 CEOs can be victimized by online masquerades," said BrandProtect General Manager Michael Kiefer. "But every duplicate account, from the CEO to the newest employee, represents a risk to the enterprise. Enterprises need to be constantly vigilant to protect their identities and reputations from becoming pawns in attacks on their executives, employees, partners, or the general public."

Masquerading and completely fictitious social media accounts are often used by cyber criminals to give legitimacy to targeted spear phishing or whaling attacks. These fraudulent accounts can also be used to drive malware or ransomware exploits against unsuspecting individuals or enterprises. Many major organizations have fallen victim to costly spear phishing schemes and BEC attacks this year including the Democratic National Convention, the Milwaukee Bucks, and the World Anti-Doping Agency. Individuals in each organization were fooled by a message from that seemed to originate from a trusted individual.

Some of these email-based attacks gain their legitimacy from the use of a trusted executive name, often presented with a link to one or more social media accounts. Many of the attacks rely on the use of a completely fictitious "executive" from a trusted company -- to make the attack seem more legitimate, these attacks may contain links to rouge social media accounts, like fake LinkedIn profiles or Twitter handles. BrandProtect threat experts recommend that all duplicative social media accounts be identified and validated. To reduce the risk of cyberattack, any unauthorized or uncontrolled accounts should be taken down.

Earlier this year, a Ponemon Institute survey sponsored by BrandProtect revealed the challenges security professionals face as they struggle to prevent external attacks. Of 591 security professionals surveyed, 64 percent of respondents felt they lacked the tools and resources necessary to monitor, 62 percent lacked the tools and resources necessary to analyze and understand, and 68 percent lacked the tools and resources necessary to mitigate external threats.

About BrandProtect

BrandProtect provides a comprehensive suite of cyber risk detection, intelligence and threat mitigation solutions for enterprises. The company deploys a unique combination of advanced proprietary

technology, overseen by a seasoned team of threat analysts, to quickly identify and mitigate fraudulent or unauthorized online activity, such as brand abuse and trademark infringement incidents, phishing attacks, mobile app schemes, Web traffic diversions, website integrity issues and defamatory discussions. BrandProtect helps security, governance, risk management, compliance and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecommunications operators and pharmaceutical companies protect their brand value and business bottom line. Learn more at www.brandprotect.com.

Contacts

For BrandProtect
Brad Puffer, 617-275-6519
bpuffer@greenough.biz