Issued 2/2/17

91% of Phishing Attacks are Display Name Spoofs

GreatHorn analyzed more than 56 million emails from 91,500 corporate mailboxes from March to November 2016. The data found that display name spoofs are the clear phishing weapon of choice for cybercriminals. Attackers are increasingly relying on highly targeted, non-payload attacks that exploit trust and leverage pressure tactics to trick users into taking action that will put their organizations at risk.

Of the more than 537,000 phishing threats GreatHorn detected in its research, 91 percent (490,557) contained characteristics of display name spoofs. Display name spoofs impersonate a person familiar to a business user in order to fool the recipient into thinking that the message came from a trusted source. It's an extremely effective tactic against a workforce deluged with incoming communications all day, every day.

Direct spoofs were the second most popular attack type (8 percent), and domain lookalikes made up less than 1 percent of phishing attacks. "Stopping spear phishing attacks isn't as simple as pushing a button; the sheer volume of these attacks, coupled with the size of the attacks surface and security resource constraints, makes it impossible to mitigate risk solely via human intervention, no matter how much you try to train your end users," said GreatHorn CEO Kevin O'Brien. "A true defense-in-depth strategy for protecting against these attacks requires unified visibility and control, coupled with risk-appropriate automation, across an organization's entire communications infrastructure."

Roughly 1 percent of all emails to business users contained email that contained specific characteristics that were deemed "risky" – a figure may seem low until the volume of emails that workers send and receive is taken into consideration. Data shows that security and IT professionals are often indecisive in how they handle a phishing attempt that has been flagged, as 41 percent take no action and only 33 percent alert an admin.