Issued 9/6/18

Hackers Increasingly Target Reputations Through Review Sites

Hackers are increasingly attempting to extort companies and individuals by threatening severe reputational harm through online reviews sites such as Yelp and TripAdvisor, security experts tell The Hill. While internet extortion schemes are not new, their perpetrators now appear to be spamming sites where enough negative reviews can scare away firms' customers. On Sunday, a group of hackers emailed CheapAir, an online travel agency, threatening to "destroy personal or company reputation online" if the company did not pay 1.5 bitcoins, roughly the equivalent of $10,000, by Wednesday. The hackers, who claimed they worked for the "STD Company," said they are "experts in destroying personal and company reputation online," according to screenshots of the emails provided to The Hill. They threatened to harm the business by posting thousands of negative reviews, replies and fraud reports on sites such as TrustPilot and Ripoff Report, as well as on social media. The cyber crooks warned that they would also destroy CheapAir's search engine ranking by spamming it with more than 1 million irrelevant blog comments such as "***** pills," according to the screenshots. "If not, we will proceed with our work and you should understand that damage once made can't be undone, not even by us," they wrote. This type of asymmetric attack — low cost, potential high impact — puts the targeted company or person on the defensive, leaving it to them to prove to negative reviews are fake to the public. Rep. John Ratcliffe (R-Texas) said extortion attacks are not a new phenomenon, but pose a growing threat to the nation's pocket as hackers methods keep evolving. In 2017, the FBI's Internet Crime Complaint Center (IC3) received nearly 15,000 "extortion-related complaints," estimating that the

financial loss of these specific schemes was over $15 million, according to the center's yearly internet crime report. Hosko, now president of the Law Enforcement Legal Defense Fund, said it is difficult to distinguish who is behind each attack. Even if federal officials stumble across digital breadcrumbs, the hackers carrying out these attacks could be halfway across the globe. Additionally, it is relatively cheap to hire hackers and services off the black digital markets to go after a company's reputation. "I found one [classical underground website] which is offering for $500 to destroy your reputation...It doesn't take $10,000 to create this. It is very cheap, unfortunately, and it is increasing right because hackers want to make profits," Wueest told The Hill. Symantec observed an interesting case recently in which a few politicians in Switzerland separately received similar emails where someone was threatening to destroy their reputations. "They actually attached a 13 page document describing all of the things that they could do. Starting from adding fake advertisements on Craigslist and similar stuff to getting bombarded with emails and phone requests, down to manipulating erotic photographs and porn," he told The Hill. While the experts interviewed by The Hill say they have not observed such attacks against U.S. politicians, they also noted that wouldn't be "surprised" if such attacks have occurred -- not all companies or individuals make the attacks against them public. Experts say internet users should be vigilant about their online activity, stating that individuals should practice safe online habits like avoiding clicking on links or attachments from unknown senders. "All of us who lower our guard are potentially at risk," Hosko emphasized.