KEEPER | PRESS RELEASE

Federal Aid May Trigger Wave of Cyberattacks on Distressed Businesses

Cybersecurity Experts Warn Attacks on Small and Medium-Sized Businesses May be Imminent as CARES Act Relief Funds are Distributed

CHICAGO, April 21, 2020 – As the federal and state agencies begin disbursing financial aid, experts at Keeper Security advise small and medium-sized businesses (SMBs) to adopt a heightened cybersecurity posture in the coming days and weeks. The warning comes amid the rollout of the $2 trillion COVID-19 stimulus bill intended to aid businesses distressed due to the outbreak of COVID-19. A **2019 study** from Keeper and the Ponemon Institute revealed that 80 percent of U.S.-based SMBs have already experienced a cyberattack.

"Coronavirus has rapidly brought on unprecedented levels of chaos, confusion and emotional distress within our nation, which creates prime conditions for cybercriminals to exploit," said Darren Guccione, CEO and Co-founder of Keeper Security. "Add in the fact that millions of Americans are working from home, using personal devices, home networks and you have a recipe for disaster."

The early stages of the pandemic revealed a number of attacks targeting the frontlines, with attacks reported against the World Health Organization (WHO) and the U.S. Department of Health and Human Services (HHS), as well as growing concern of ransomware attacks that could cripple hospitals. But experts say the next wave of attacks may be inspired by financial opportunity associated with the stimulus measure. Guccione believes that federal aid, grants and small business loans could be a near-perfect catalyst to incentivize online scammers to strike. Attacks of this nature will not require sophisticated tactics to be effective and may largely rely on user error or deception, such as email phishing campaigns. Guccione also predicts that stolen credentials on the dark web will be more frequently utilized by cybercriminals to execute credential stuffing and account takeover attacks.

Keeper's **2019 Global State of Cybersecurity in Small and Medium-Sized Businesses** found that two of the most common attacks used against SMBs were phishing (57%) and credential theft (30%). Cybercriminals can easily mask an email to appear as if it's coming from a friend, colleague or government agency, offering a compelling reason for a user to click on a link. Once a link is engaged, there is little to no recourse a user can take to avert the hack. Beyond financial consequences, the study also found that 69 percent of global respondents lost sensitive information due to an attack, which can cause irreparable harm to an organization's reputation.

The virus outbreak is also stretching the utilization of government-backed resources, offering fewer government safety nets to fall back on in the face of online fraud or cyberattack. Many SMBs struggle to rebound from cyberattacks under normal economic circumstances, making the coming months extra perilous for this segment of the business. Keeper advises businesses to be extra vigilant when handling online communications and inform employees of the heightened risk, noting that the best defense is a proactive approach to security.

The pain felt from economic turmoil isn't limited to American SMBs and neither is the elevated cybersecurity threat. Similar to the U.S., the U.K. and countries in Europe have also rolled out coronavirus financial aid packages for businesses. Globally, two-thirds of SMBs experienced an attack within the 12 months prior to responding to Keeper's survey. Further, respondents said those attacks are becoming more frequent, targeted and sophisticated.

"Tools like password managers and VPNs provide businesses with an extra layer of protection against user error but there's no better solution than a proactive approach to digital security," said Guccione.

KEEPER | PRESS RELEASE

The **2019 Global State of Cybersecurity in Small and Medium-Sized Businesses** report, which surveyed 2,391 IT and IT security practitioners in the U.S., U.K., DACH, Benelux and Scandinavia, underscores growing cybersecurity concerns best illustrated through the year-over-year trends dating back to 2016.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com.**