KEEPER | PRESS RELEASE

Keeper Security Issues Warning About Heightened Ransomware Attacks Amid COVID-19 Pandemic

Keeper offers educational resources to help businesses protect themselves as ransomware attacks surge

CHICAGO, Sept. 9, 2020 – Keeper Security, provider of the highly-rated cybersecurity platform for preventing password-related data breaches and cyberthreats, today issued a statement regarding the heightened risk of ransomware attacks. Such attacks surged 25% in the first quarter of 2020 and are continuing to grow in frequency amid the COVID-19 pandemic. To help organizations navigate the current ransomware threat landscape, Keeper today launched its online **Ransomware Center** with educational resources, including a ransomware whitepaper outlining the risks and offering prevention strategies.

“Ransomware attacks have become one of the most urgent threats businesses face today,” said Darren Guccione, CEO and Co-founder of Keeper Security. “The massive social and economic disruptions converging this year are creating the perfect environment for cybercriminals to exploit and ransomware is their cyberweapon of choice. We are urging businesses to educate themselves, take advantage of free resources available to them and implement additional cybersecurity protections immediately.”

Even before the COVID-19 pandemic, ransomware was on the rise. Global damages from ransomware attacks more than doubled between 2017 and 2019, from $5 billion in 2017 to $11.5 billion in 2019. Damages are expected to reach $20 billion by 2021. Keeper will host a webinar with world-renowned cybersecurity expert Dr. Eric Cole to discuss “How to Mitigate the Risk of Ransomware Attacks” on Tuesday, September 15 at 1:30pm (CDT). To register for the event, click **here**.

Keeper’s Ransomware Center offers organizations free resources and strategies to help prevent a ransomware attack. The whitepaper, Understanding & Preventing Ransomware Attacks, details the risks associated with ransomware attacks, outlines the industries that are the most vulnerable and addresses the great debate of whether to pay the ransom. Other resources include access to the live webinar, a downloadable infographic and strategies for businesses of all sizes to protect themselves from ransomware attacks, which include:

1. **Performing regular system backups.** Regular backups are essential, not only to recover data after a cyberattack, but also after system outages or damages to hardware after natural disasters.

2. **Training employees to avoid phishing and other scams.** Given that many ransomware attacks start from phishing emails, training employees on how to detect and avoid phishing scams is key to prevention.

3. **Securing employees’ passwords.** The overwhelming majority of data breaches can be traced back to poor employee password habits. Enforce strong password hygiene by mandating usage of strong, unique passwords for all accounts, multi-factor authentication (2FA), and a password manager.

4. **Subscribing to a dark web monitoring solution.** On average, it takes companies over 100 days to realize they’ve been breached, but a dark web monitoring service notifies businesses if an employee’s credentials have been trafficked on the dark web in real time.

All statistics cited in this release can be referenced in Keeper Security’s whitepaper **Understanding & Preventing Ransomware Attacks.**

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented 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**.