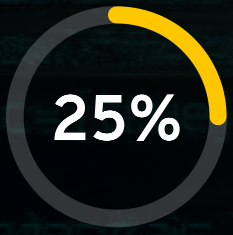
KEEPER
Cybersecurity Starts Here®

Understanding & Preventing RANSOMWARE ATTACKS

REV 8.18.20



increase in ransomware attacks between Q4 2019 and Q1 2020

of victims gave into ransom demands in 2018

of victims gave into ransom demands in 2020

INTRODUCTION

Ransomware is a type of malware that encrypts a computer's files, locking users out of the system until a ransom is paid to a cybercriminal, usually in bitcoin. Ransomware attacks have become increasingly common for **three reasons:**

- They require little technical expertise to launch. Less technically sophisticated attackers can even purchase "ransomware-as-a-service" packages on dark web forums.
- Unlike data breaches, where cybercriminals must first steal data, then find willing buyers, ransomware paydays are almost immediate.
- More victims than ever are paying up. In 2018, only 39% of victims gave into ransom demands; by 2020, that figure was estimated to be as high as 58%.[1]

Ransomware attacks are rapidly increasing in frequency, with a surge after the COVID-19 pandemic began. Between Q4 2019 and Q1 2020, ransomware attacks rose by 25%,[2] and ransomware finally surpassed payment card theft to become the most common type of cyber threat.[3] A new attack happens about every 14 seconds.[4]

> **A new attack happens about every 14 seconds.**

SOURCES:
[1] Security Boulevard [2,3] Ciodive [4] Cybersecurity Ventures

THE HIGH COST OF RANSOMWARE ATTACKS

The financial toll from ransomware attacks is also rising. Global damages from ransomware attacks more than doubled between 2017 and 2019, and they are expected to reach $20 billion by 2021.[5] In addition to direct costs, such as ransom payments and repairs to damaged systems, organizations face significant indirect costs from having to scale back operations or temporarily close while repairs are made. The average downtime from a ransomware attack is 9.6 days.[6]

> Global damages from ransomware attacks more than doubled between 2017 and 2019, and they are expected to reach $20 billion by 2021.

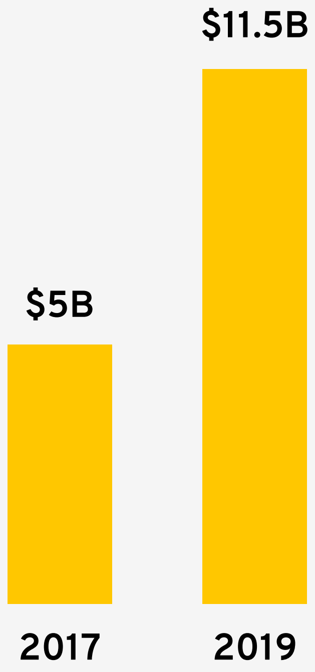
While cyber insurance covers some of these costs, organizations cannot depend on cyber policies to make them whole after a ransomware attack. The typical cyber insurance policy does not cover regulatory fines for violating compliance mandates such as PCI DSS and HIPAA; attacks involving malicious insiders, including disgruntled employees, ex-employees, and third-party vendors; or all of an organization's losses from downtime.

If an organization must shut down for an extended period of time, or if digital, intellectual property (IP) is breached during the attack, it could suffer irrevocable damage.

The Emerging Threat of Double Extortion

Double extortion, also known as "name and shame," effectively transforms ransomware attacks into data breaches. After first appearing in late 2019, it now accounts for over one-tenth of ransomware attacks.[7] In a double extortion attack, cybercriminals don't just encrypt a victim's data; they also steal it, then threaten to publicly release or sell it if the ransom is not paid.

Ransomware Damages Rose 230%



SOURCES:
[5] Cybersecurity Ventures [6] Dark Reading [7] Health IT Security

HIGH RISK SECTORS

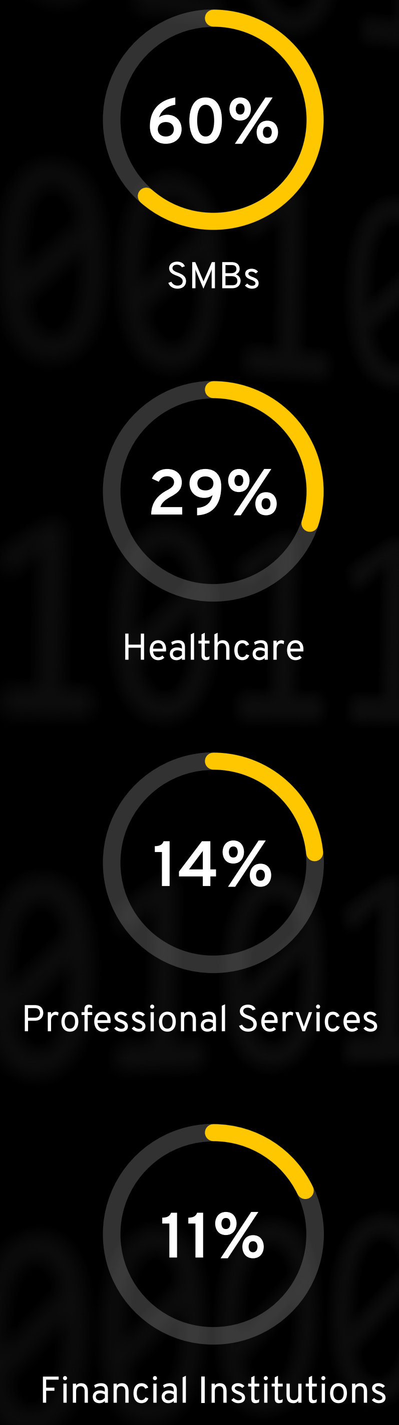
When ransomware first emerged, victims were usually very large enterprises; the reasoning was that these victims had deep enough pockets to pay ransom demands. However, large companies could also afford to harden their security defenses to prevent future attacks. Stymied by comprehensive cybersecurity defenses at large enterprises, cybercriminals turned their attention to small and medium-sized businesses (SMBs) and state and municipal governments. These organizations tend to be resource-poor. Nearly half of private-sector SMBs budget less than $5,000 per year on cybersecurity,[8] and most U.S. states devote less than 3% of their budgets to IT security.[9]

In 2019, SMBs represented about 60% of ransomware victims, with healthcare, professional services, and financial institutions the top three targets.[10] Ransomware attacks on healthcare organizations surged by 350% between 2018 and 2019,[11] and most successful attacks target facilities with fewer than 500 employees.[12]

Ransomware incidents targeting municipal governments rose by 60% in 2019,[13] when over 163 ransomware attacks hit municipal governments around the U.S. Victims paid at least $1.8 million in ransom, in addition to tens of millions more in recovery and mitigation costs.[14]

> **Ransomware incidents targeting municipal governments rose by 60% in 2019.**

Which sectors are most at risk?



SOURCES:
[8] StorageCraft [9] Ciodive [10] Ciodive [11] Becker's Health IT
[12] Health IT Security [13] MSSP Alert [14] Dark Reading

CYBERCRIMINALS ATTACK LARGE ENTERPRISES' SUPPLY CHAINS

This is not to say that large enterprises are immune from ransomware attacks. The first half of 2020 saw a spate of attacks on major corporations, including Honda, Chubb, Cognizant, Garmin, and U.S. Department of Defense contractor, CPI. Garmin is rumored to have paid $10 million to regain access to its systems.[15]

Today's sprawling supply chains are another route through which cybercriminals attack large enterprises and multinationals. If a cybercriminal cannot get past a large enterprise's security defenses, they target a small, resource-poor vendor. In March 2020, an organized cybercrime group used DopplePaymer ransomware to attack a supplier for Tesla, Boeing, and Lockheed Martin.[16] Three months later, the same group targeted an IT contractor whose customer roster included NASA and a number of Fortune 100 firms.[17] In May 2020, another organized ransomware group targeted two food distributors to national supermarket chains, including Kroger, Sprouts, and Albertsons.[18]

> “
> **Today's sprawling supply chains are another route through which cybercriminals attack large enterprises and multinationals.**

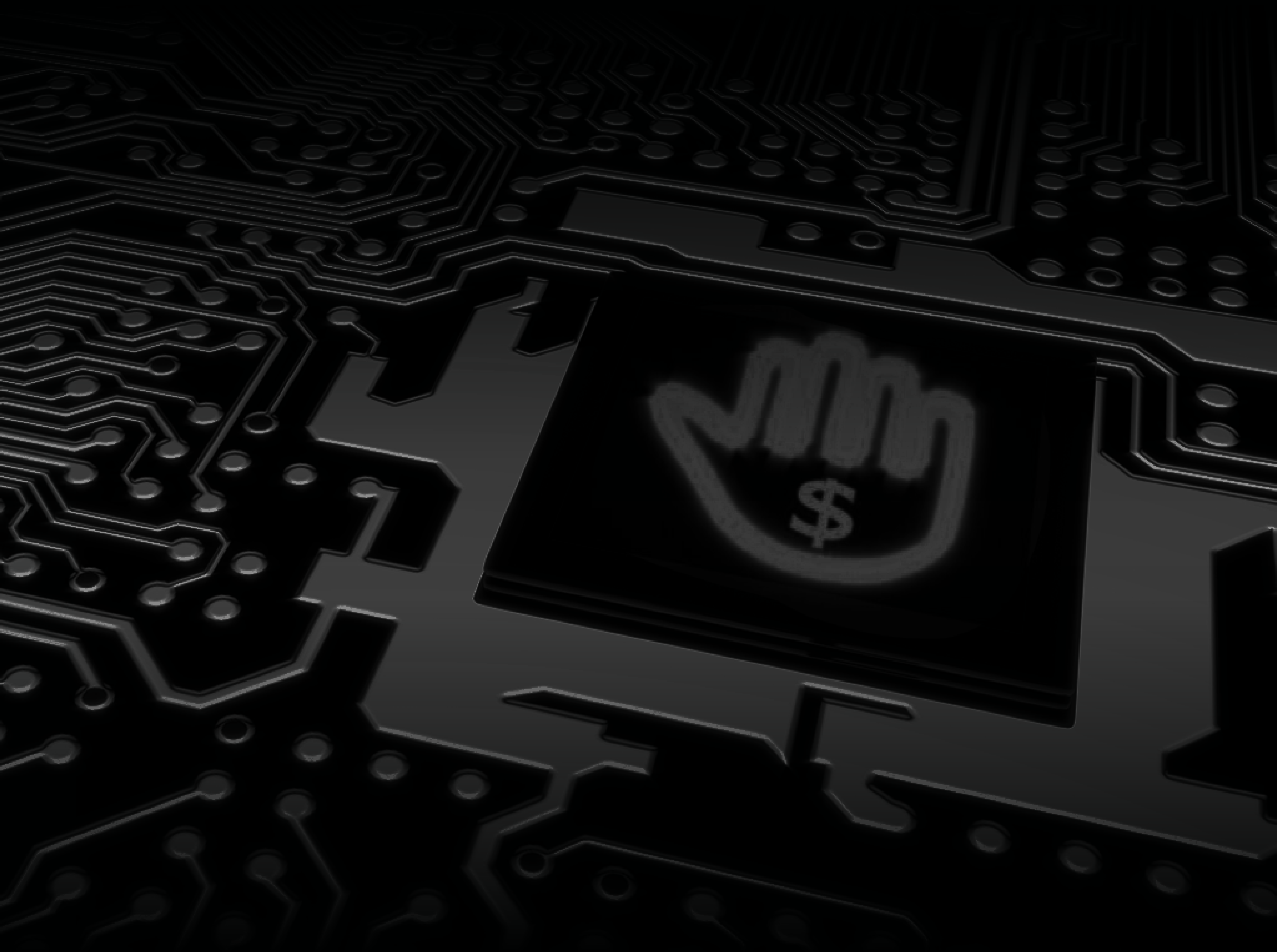
SOURCES:
[15] Wired [16] Ciodive [17] CPO Magazine [18] MSSP Alert

RANSOM: TO PAY OR NOT TO PAY?

Whether to pay a ransom is a matter of great debate, even among cybersecurity professionals. Cyber insurers often encourage victims to pay; most policies cover ransom payments. Some security professionals argue that ransom costs may be far lower than data recovery costs, especially for SMBs that cannot afford extended downtime. At healthcare facilities and government agencies, downtime could put human health and lives at risk.

Other security professionals, as well as most law enforcement agencies, argue that paying ransoms only encourages future attacks, and paying does not guarantee restoration. While most organizations that pay up do get their data back, approximately 20% do not.[19] Additionally, in double extortion cases, cybercriminals still have possession of stolen data. Regardless of their promises to destroy the data after receiving the ransom, they may still sell it, publicize it, or use it as fodder for future attacks, such as business email compromise (BEC).

With so much at risk, the optimal solution is to prevent ransomware attacks from happening in the first place.



SOURCES:

[19] GCN

HOW TO PREVENT RANSOMWARE ATTACKS
(1 OF 2)

Antivirus software and most identity and access management (IAM)systems do little to protect organizations from ransomware. Ransomware defense requires a multi-pronged, proactive approach.

Perform Regular System Backups

Regular system backups are essential, not only to recover data after a ransomware incident or another cyberattack but also after catastrophic system outages and damage to hardware after natural disasters. However, system backups are not a silver bullet, as new-gen ransomware variants seek out and encrypt backup files before attacking the rest of the network.

Train Employees to Avoid Phishing & Other Social Engineering Scams

Since many ransomware payloads are delivered in phishing emails, training employees to avoid phishing scams is another critical step to preventing infection. However, like system backups, it is not a silver bullet, as brute-force attacks have surpassed phishing to become the most common method of delivering ransomware.[20]

> “
>
> **Ransomware defense requires a multi-pronged, proactive approach.**

SOURCES:
[20] ZD Net

HOW TO PREVENT RANSOMWARE ATTACKS
(2 OF 2)

Secure your Employees' Passwords

Weak and compromised passwords are the biggest threat to organizational cybersecurity. In addition to fueling the brute-force attacks that are the most common ransomware delivery method, poor employee password habits are behind the overwhelming majority of data breaches.

In a brute-force attack, cybercriminals obtain a list of passwords stolen during a data breach, then attempt to use them to compromise servers and endpoints, usually with the aid of bots. Because so many users use weak, common, and easily guessed passwords, and reuse passwords across accounts, these attacks are very successful. Brute-force attacks can be prevented by mandating that employees use strong, unique passwords for all accounts; use multi-factor authentication (2FA) on all accounts that support it, and use a password manager.

Subscribe to a Dark Web Monitoring Solution

Even if a user is diligent about using strong, unique passwords, their password can still be compromised. Data breach victims are typically the last ones to know that their passwords have been stolen. The average "dwell time," which is the period between the initial breach and the time a company discovers it, is 101 days.[21] Dwell times that greatly exceed this average are not unheard of. It took Marriott Starwood four years to discover that its systems had been breached.[22] Once cybercriminals steal login credentials, they put them to use very quickly.

For this reason, Dark Web monitoring services are essential to preventing ransomware infections. These services scan Dark Web forums and notify organizations in real-time if any of their employee passwords have been put up for sale, allowing IT administrators to force password resets right away.

SOURCES:
[21] Dark Reading [22] Ibid

HOW KEEPER HELPS ORGANIZATIONS PREVENT RANSOMWARE ATTACKS

Keeper's zero-knowledge password management and security platform provides organizations with complete visibility into employee password practices, enabling IT administrators to monitor password use across the entire organization and enforce the use of strong, unique passwords, 2FA, role-based access control (RBAC), and other security policies. Keeper also supports multiple compliance standards, including HIPAA, DPA, FINRA, NCUA, and GDPR.

Each employee receives a private, encrypted digital vault that they can access from any device using one master password -- the only password the employee will ever have to remember. Keeper's password manager generates strong, unique passwords for every account and automatically fills in login fields on websites and apps. Employees no longer have any reason to reuse passwords or use weak passwords, and IT administrators have the visibility they need to ensure compliance with the rules.

IT administrators can fully customize employee permissions through fine-grained access controls based on their roles and responsibilities, as well as set up shared folders for individual departments, project teams, or any other group. For enhanced protection, organizations can deploy valuable add-ons such as Keeper Secure File Storage, which enables employees to securely store and share documents, images, videos, and even digital certificates and SSH keys, and BreachWatch™, which scans Dark Web forums and notifies IT administrators if any employee passwords have been compromised in a public data breach.

Keeper takes only minutes to deploy, requires minimal ongoing management, and scales to meet the needs of any size organization. Keeper's business and enterprise password management solutions help thousands of companies all over the world prevent password-related cyberattacks, improve productivity, and enforce compliance.

> **“Keeper's business and enterprise password management solutions help thousands of companies all over the world prevent password-related cyberattacks, improve productivity, and enforce compliance.**