AN SMB **QUICK GUIDE** FOR OVERCOMING TODAY'S CYBERATTACKS

SURVIVING THE RISE OF RANSOMWARE

Introduction

What is a business's most valuable asset? Is it the fixed assets? The workforce? The established business relationships with clients and other partners? It may be none of these things. In 2022, the company data is likely the most valued asset.

The value of data has never been higher. In fact, some analysts have posited that for many companies, the value of their data is greater than the value of the company, according to Douglas B. Laney, writing for Forbes magazine.

This reality, of course, has led to SMBs investing in people, processes, and technology to protect their data from theft. And while data theft — in which hackers swipe customer data to empty bank accounts or file fraudulent tax returns — is still a legitimate risk, many hackers find it more lucrative to simply hold the data hostage using ransomware.

Since ransomware is software that encrypts a company's data on a computer or network and locks it up in a way that's impossible to unlock without an encryption key, so it is like a digital hijacking. It's followed by demands for payment to regain access to critical data and operations and is sometimes so sophisticated that the bad actors offer customer service to those who have had their data hijacked. Many companies are dead in the water while they're under attack from ransomware. They are often obligated to pay extortion money to the attackers if they ever hope to use their data again and resume normal operations.

“In previous years, as investors clawed for scraps at Sports Authority’s and Radio Shack’s ‘going out of business’ sales, the highest bidders were not interested in their inventories of jockstraps and joysticks, but rather in their customer data.”

Ransomware is on the Rise

According to a recent study by ThoughtLab, the average number of cyberattacks and data breaches increased by 15.1% from 2020 to 2021.

Security analysts have noted that the pace of attacks will likely accelerate due to social engineering and ransomware as malicious nation-states, organized crime groups, and lone wolves become more sophisticated. At the same time, 29% of CEOs and CISOs and 40% of chief security officers stated that their organizations are unprepared for this new threat landscape.

For developers who create ransomware software for their own use, the only way to achieve a return on investment is to use the software themselves, which involves a number of risks or sell it for a high price to organized cybercrime groups. Potential targets may be harder to attack today because businesses are more aware of the threat and have taken steps to mitigate them. And while it’s difficult for law enforcement to arrest and prosecute individuals or groups engaging in ransomware attacks, it does happen on occasion.

So how does a shady developer earn money on a sophisticated ransomware solution? By turning it into a service and essentially renting it out to anyone who wishes to perpetrate ransomware attacks but doesn’t have the IT know-how to create a solution of their own. In addition to a monthly fee for the use of the solution, ransomware developers can demand a portion of the ransom users receive — typically between 20% and 30%.

What is Ransomware as a Service?

The costs of a RaaS solution are negligible compared to the “value” criminal actors can reap from ransomware: the 2021 CrowdStrike Global Security Attitude Survey revealed that the average ransom demand in 2021 was $6 million.

Ransomware as a service (RaaS) is a criminal business model in which ransomware creators and operators essentially charge “clients” or affiliates for the use of ransomware tools. Essentially, it’s a way to outsource the crime of ransomware attacks using the software as a service (SaaS) business model. It removes the barriers to engaging in ransomware attacks, as it can be purchased for a modest sum by anyone who visits the dark web marketplaces where it’s marketed and sold.

RaaS, developed by organized crime syndicates, is a lucrative business. It follows the SaaS model in several ways. Developers often sell RaaS “kits” that include round-the-clock tech support, bundled products and complementary technologies, user reviews and forums, and other benefits typically offered by the providers of SaaS solutions. Payment for services is often rendered in cryptocurrency to avoid detection by law enforcement. Many ransomware creators even employ expert negotiators so users can tap their expertise in communications with victims. Some RaaS creators allow their users to access dashboards that sum up total payments from victims and the total number of files successfully encrypted.

.

The Colonial Pipeline Attack: RaaS in Action

In May of 2021, the Houston-based oil pipeline system Colonial Pipeline suffered a ransomware attack on the computerized equipment that controls the pipeline carrying gasoline and jet fuel to the American Southeast. Colonial Pipeline provides about 45% of the fuel used on the U.S. east coast. The attack, carried out using a RaaS solution by the criminal hacking group DarkSide, shut down all pipeline operations and brought fuel delivery to a halt, forcing many airline companies to cancel flights. The ransom money (75 bitcoin, or about $4.4 million at the time of the attack) was paid by Colonial Pipeline under the guidance of the FBI. The company was able to resume most operations by the end of the week but not before causing fuel shortages, a rise in local gas prices, and panic buying. Ultimately, the U.S. Department of Justice was able to claw back about $2.2 million of the ransom money.

SMBs Need to Prepare for a Surge in Ransomware Attacks

Without significant preparation, disruptions from ransomware attacks are likely to become more severe in the coming years.

Most global organizations — large companies, as well as SMBs— are still highly vulnerable to these types of attacks, and the proliferation of ransomware as a service solutions will enable most hackers — even those without IT expertise of their own — to try their hand at a ransomware attack. Traditional backup without expert business continuity and incident response plans are not enough to prevent or quickly recover from attacks.

While many small business operators may believe that they are too inconsequential to be a target for ransomware, this is demonstrably not the case. Hackers often seek softer targets that may be less prepared for an attack. And while large companies can sometimes weather the ransom payment, the results can be catastrophic for a small and growing business. In addition, while the costs of development for traditional ransomware software meant large targets were more desirable as marks, RaaS solutions allow even minor criminals to target smaller businesses lucratively.

Managed service providers, like us, can use a multi-layer strategy approach to keep their clients safe from potential ransomware attacks. This strategy includes a combination of:

This strategy includes a combination of:

- Malware protection
- Rock solid data backup
- Digital rights management
- Encryption
- Tools such as VPNs and reliable endpoint protection
- Software patches
- Firewall protections against malware for cloud networks
- DNS security to detect websites that could host malware,
- And multi-factor authentication to stop hackers from launching a ransomware attack from a stolen password
- Business continuity tools to enable business as usual in the event of a recovery

> It is critical to make absolutely certain your backup and disaster recovery solution has ransomware protection and that you can know your team will have true business continuity if you are attacked.

Thwart Ransomware and Protect Everything with Business Continuity

Data Protection and Recovery for Desktops, Laptops, and Workstations

Our backup and disaster recovery solution saves and protects your data so it can be restored in the event of a malicious or accidental deletion or encryption attempt. This is called AirGap. It's your last line of defense when there's a cyber-attack on your backup files. Here's how it works...

The chain-free Business Continuty platform creates a gap – in the form of a time delay of the deletion request – between the actual filesystem and the recovery solution. The backup and disaster recovery and business continuity (BCDR) tool continuously takes native snapshots of your filesystem and keeps them in a safe location separate from your actual filesystem. Hackers are tricked into thinking they've found the filesystem root and backup files, but in reality, you're safe! AirGap ensures that hackers targeting backup files do not obtain access in the first place, with multiple validations required to delete Protected System backups.

As a built-in enhancement to your BDR solution, AirGap creates a secure environment that makes data destruction nearly impossible – whether from a ransomware attack or any other type of disaster.

Most importantly, our Disaster Recovery quickly restores your Protected Systems in as few as 15 minutes. That near-instant recovery eliminates the stress, financial burden, and loss of business caused by downtime.

The Benefits of Business Continuity with AirGap for SMBs:

1. **Cost-effective:** Significantly increase your MSP (and BCDR) return on investment (ROI) by eliminating the risk of ransomware and potential ransom payments, data loss, regulatory fines, downtime costs, and damage to your business reputation.

2. **Preventative:** Reduce accidental deletions and ransomware threats with multiple validations required to delete Protected System backups.

3. **Worry-free:** Your data is safe no matter what with native snapshots of Protected Systems stored in a safe location, separate from your actual filesystem.

4. **Almost instant recovery:** Quickly get back to business with one call to our Help Desk.

Contact us to learn more today!