US SIGNAL®

10 TIPS
TO COMBAT RANSOMWARE

TABLE OF CONTENTS

THIS IS WAR

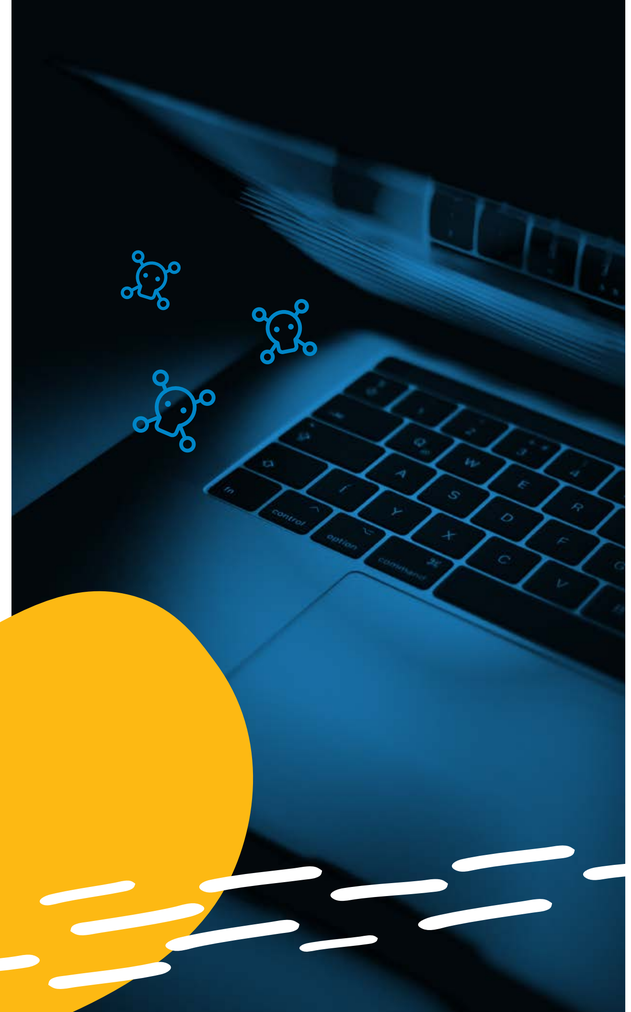
There's a battle raging. It's ransomware versus IT, and the stakes are high.

Cyber attackers are employing increasingly sophisticated means to infect computers with viruses that hijack data by encrypting it. It's only returned once a ransom is paid. At risk: the systems and data that power all aspects of business operations.

Every day the headlines are touting the exploits of WannaCry, Petya, NotPetya, CrytoLocker, Satan, Reyptson, Locky and other ransomware families and their variants. Not only are the operators behind them enjoying a successful surge. They are diversifying their attack tactics to hit more potential victims, platforms, and bigger targets.

If some of the biggest organizations around the world — with equally big security budgets and resources — are falling victim to ransomware, is there any hope for the average SMB?

The answer is "yes" if you adopt a multi-faceted defense strategy comprised of best practices and practical measures to repel ransomware attacks and mitigate their effects if they do occur.
Read on for US Signal's top 10 tips for winning against ransomware.



1. KNOW WHAT YOU HAVE AND WHAT YOU DON'T

Companies don't fall victim to ransomware by accident. Think about what's at risk if your IT systems are hijacked. What data is most valuable to your business? Where does it reside? Who touches it and when? When was the last time you had vulnerability scanning or a penetration test conducted? How is accessibility managed? What would happen to your business if it was compromised?

Are there holes in your organization's IT defenses? Do you have an Incident Response (IR) plan? Does your BC/DR plan account for backing up and recovering data in the event of a cyber attack? Have you tested your IR plan or BC/DR plan?

At a minimum, conduct tabletop exercises with your organization's leaders and the IT and Security teams that are responsible for responding to ransomware incidents. Consider using a third-party expert to help you identify gaps and develop solutions to keep all types of malware at bay.

2. BACK UP TO STAY UP

Back up your most important data every day. If your IT systems get locked up, you can restore your system from a clean backup. You'll avoid paying a ransom to see your data again and eliminate the potential for business-disrupting downtime.

Note: Ransomware can encrypt files on mapped drives. Only back up to an external drive or backup service that isn't assigned a drive letter or is at least disconnected when not performing backups.

Use the 3-2-1 approach to backup:

3 **Make three copies of your data so that your original data is supported by two separate backup copies.**

2 **Use two different media formats to reduce the chances that all possible avenues of recovery will be inaccessible through equipment failure.**

1 **Keep a copy offline (air gapped) so that attackers can't gain access to it.**

3. INCREASE YOUR RESILIENCE WITH DRaaS

Backups are essential, but they aren't enough. Increase your organization's resilience with a Disaster Recovery as a Service (DRaaS) solution.

DRaaS enables you to quickly failover your production systems by spinning up VMs in minutes as opposed to restoring files from a clean backup that can take four to five hours on a good day. If ransomware attacks, rather than paying a ransom in exchange for an encryption to free up your data, you can quickly switch production environments and keep operations running like normal.

Plus, with DRaaS, admins can boot a production server and immediately verify whether the application is infection-free. If it successfully boots, then you have a clean image.

4. PREPARE EMPLOYEES FOR BATTLE

Employees are often the first to encounter ransomware; they may even be the cause of it. Counter that by making them your first line of defense.

Start with frequent security training.
Educate employees about the various types of threats they may encounter — including ransomware hidden in emails — and what they should do. Why the big deal about emails? Approximately one in five users will click on a bad link in an email, enabling bad actors to sneak into your system.

Consider adopting a phishing assessment program to evaluate the effectiveness of your security awareness training. There are many low-cost or no-cost options available. Use the results to improve your organization's awareness training.

5. CENSOR. STRIP. RELEASE.

They look innocent. But, as noted in Tip #4, emails can provide the opening for ransomware to hijack your data. It's not just the links they may contain; malicious files can be a problem too.

Don't wait for an unsuspecting employee to open a ransomware-loaded email attachment. Configure your mail servers with "allow lists" to only permit only the sending or receiving of file types critical to your business. Allow lists take more work to configure but provide better protection than block lists. Files with EXE, COM, SCR JAR BAT or JS extensions should not be allowed through. The files should be stripped or quarantined before any email containing these file types can be delivered to its intended recipient.

You can also automatically quarantine Microsoft Office document attachments that contain macros, another ransomware distribution method. Consider quarantining all attachments, regardless of type. Hold them for approval before releasing them to the designated recipient.

6. LIMIT PRIVILEGES AND PERMISSIONS

When ransomware infects a computer, it uses the “permissions” of the user logged on. What that person can access, the ransomware can access. Put an end to that by restricting your system users’ privileges and network drive connectivity.

Only grant access to the folders each user requires for performing his or her job. Also make sure to restrict users from being local administrators on their workstations.

You can also limit what attackers can access by logically segmenting network assets, resources, servers and workstations. By utilizing network segmentation or internal firewalls, only approved types of communication flow between devices limiting the ability of ransomware to spread.

With restricted access between segments, an attacker’s movement from one to another will be halted, or at least slowed down enough, so that monitoring tools can alert your staff of the intrusion.

7. GET BACK TO THE BASICS

Endpoint antivirus solutions aren’t glamorous, but these basic security tools can be effective for initial ransomware detection. Implement multi-factor authentication (MFA) for all remote logins, VPNs, and cloud accounts.

Upgrade from traditional antivirus to an endpoint detection response (EDR) or extended detection response (XDR) solution. They ensure your endpoints are up to date with the latest defenses and give you the ability to remotely quarantine or isolate an endpoint if problems arise. Make sure your servers and file shares are protected by an EDR or XDR solution as well.

Deploy an email security gateway product that defends against spam, phishing, and email-based malware before the email ever reaches your end user.

Supplement with firewalls that use explicit “allow listing,” have IPS and IDS, and utilize robust blocklisting for things like DNS-based threats and malicious web links. They can help reduce the likelihood of successful web-based malware downloads and deter ransomware from connecting to command-and-control servers.

8. ENAGE IN “PATCH” WORK

Nothing is perfect, especially software that is released iteratively and often. Hence, software manufacturers are continually releasing updates and patches to take care of newly discovered issues. But, ransomware operators are counting on you not to keep your software up to date so they can exploit vulnerabilities that allow them to sneak into your system. Foil them by adopting an aggressive patch management policy.

Update your software often. Utilize a vulnerability scanning platform and monitor manufacturer and industry security alerts. Apply patches on a timely basis. This is not the time to say, “I’ll do it tomorrow.”

Enable automatic updates whenever possible or consider a patch management software platform. Or, go directly to the vendor’s website. If vulnerability scanning and patch management are too much of a hassle, outsource the tasks to a managed service provider.

9. IT'S YOUR DOMAIN

Initial DNS resolution by ransomware relies on the domain generation algorithm (DGA). This makes blocking known bad domains difficult because the DGA can use thousands of different domain names to reach the command-and-control server. Nonetheless, increasing visibility into your domain names servers (DNS) can be useful when you're dealing with an incident and for providing an early warning system.

Consider using security features on your DNS servers or firewall to block things like newly created domains or known malicious domains. Consider a cloud-based firewall solution that has built-in DNS security features to help protect your business.

10. EN GARDE!

If your company is the victim of ransomware, act immediately. Remove the infected computer from your networks to keep it from continuing the encryption process and to limit ransomware from spreading to other systems. Consider disconnecting network segments at the physical switch to minimize spread or contain the impact of the ransomware.

If you use Common Internet File System (CIFS) /Server Message Block (SMB) on other operating systems, the ransomware will see them as Windows shares. Protect them as well to reduce the chance of these shares being encrypted.

Important next step: identify the specific variant. You must know what you're up against before you contain it. If you don't have internal expertise, seek outside professional assistance. Consider disconnecting network segments at the physical switch to minimize spread or contain the impact of the ransomware.

HAPPILY EVER AFTER... **FOR NOW**

Follow these tips to help you dodge the bullet of a devastating ransomware attack. But keep in mind that the most well-regimented patch management processes, the most technically advanced anti-virus tools, and all other tactics are merely that: tactics. The people behind ransomware are relentless. They will do everything they can to stay a few steps ahead of the anything you do to protect your data – or at least everything they can to maneuver around your policies and processes.

Never let your guard down. Winning the war against ransomware requires constant vigilance — and doing whatever you can to fortify your position. That includes calling in the reinforcements, like US Signal.

ABOUT US SIGNAL

Learn how US Signal can help you safeguard your business assets from ransomware and other malware, pre-emptively detect security gaps mitigate data loss if a disaster occurs, and keep mission-critical applications operational.

US Signal offers a comprehensive service portfolio of disaster recovery and business continuity options to ensure data availability while mitigating IT-related business disruptions. All services are powered by the company's own resilient private fiber network and PCI- and HIPAA-compliant infrastructure.

For more information, call 866.2.SIGNAL or email info@ussignal.com.

US Signal is audited for compliance with or holds certifications for numerous regulatory requirements and industry standards. Among them:

HIPAA COMPLIANT · PCI · AICPA SOC · AICPA SOC 2 · 2021 CJIS READY · ITAR COMPLIANT INTERNATIONAL TRAFFIC IN ARMS REGULATIONS · GDPR