ISSUE 29 SPRING 2020

Newsletter

What's Inside

Your Next Ransomware Attack May Require Two Payments
Page 01

Buying Antivirus Software?
Page 02

Stay Afloat During the Pandemic: 5 Useful Tips
Page 03

Monthly Tips
Page 04

Your Next Ransomware Attack May Require Two Payments!

In a case of adding insult to injury, a new strain of ransomware is looking for one payment to decrypt, and a second payment to not publish stolen files.

We first saw the Maze ransomware late last year first threaten the release of victim data should the ransom not be paid. In recent months, it seems nearly every ransomware strain has jumped on board and are utilizing this new money-making practice.

But a new twist has surfaced with Ako ransomware. In addition to holding data for ransom and stealing data, threatening to publish it if the ransom isn't paid, Ako also has demanded a second ransom to not release the stolen data. This tactic appears to only apply to larger victim companies and is also dependent upon the kind of data stolen.

While we've seen the average ransom doubling this year, this second demand for a ransom tends to run in the $100K to $2M range (remember, the organizations seeing these types of attacks are the ones the the Ako folks believe have deep pockets). This second ransom almost assures the cybercriminal some form of payment, one way or another.

Ransomware-turned-data breach is the name of the game moving forward.

The only good answer here is to strengthen every weak point in your organization's security. Security solutions will help, but the user themselves needs to be equally more security-minded. Enrolling them in continual Security Awareness Training will lower the risk of falling for a phishing attack or social engineering scam that results in the installation of ransomware.

There is a reason more than half of today's ransomware victims end up paying the ransom. Cyber-criminals have become thoughtful; taking time to maximize your organization's potential damage and their payoff.

After achieving root access, the bad guys explore your network reading email, finding data troves and once they know you, they craft a plan to cause the most panic, pain, and operational disruption. Ransomware has gone nuclear.

Written by Stu Sjouwerman at KnowBe4.

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

Buying antivirus software? Consider the following points:

You probably didn't need to worry about antivirus protection before. At the office, the IT department handled it. At home, your personal setup may not contain enough valuable information to warrant industry-strength. But because of the global pandemic forcing most of us to stay indoors, your home is now your office, too. If you're looking to boost your antivirus software, keep the following in mind.

Not all antivirus software solutions are the same. If you're considering getting one, you need to identify what you and your company needs. Then do your research among the available options in the market. Here are a few things to consider when you shop for antivirus software.

#1 Cost

There are free-to-use antivirus software products in the market, but they only offer basic protections that seasoned hackers can easily infiltrate. You'll need to pay in order to upgrade and enjoy full protection. And there's a danger that the free software contains adware, or that it collects data and sells them to third parties.

Nowadays, nothing's for free. The good news is that protection need not be expensive. If you partner with a managed IT services provider like us, we'll figure out the right protection based on your needs and budget.

#2 Speed and performance

Not long ago, antivirus software consumed a lot of computer memory and slowed down devices. But thanks to new technology, the problem of speed has been addressed. Still, antivirus performance should take precedence over speed. What's the point of a fast computer if it's vulnerable to hackers and malware?

#3 Compatibility with multiple devices

These days, most people use or own more than one device, such as smartphones and tablets. Look for antivirus software that can protect all your devices, regardless of software version or date of purchase. It'll be inconvenient and expensive to have different security software per device.

#4 Comprehensive protection

Your antivirus should protect your devices from a wide variety of threats. These should include popular malware and phishing attacks, as well as malicious downloads, denial-of-service (DoS) attacks, cryptojacking, and other damaging threats.

#5 Customer support and service

Take some time to learn more about the antivirus software manufacturer. Does the company have a solid reputation? Are they at the forefront of developing solutions against looming threats? Are they responsive to the changing cyberthreat landscape? And are they customer-driven? If they tick all the boxes, you're sure that their products and services are worth your investment.

Cybersecurity is not a luxury but a necessity for all businesses. If you're looking for the right antivirus protection, then let our experts help you. We'll provide you with the robust security your devices and network need.

FEATURED PARTNER

tenable®

Tenable is founded on 1 simple concept: minimize cyber exposure. Starting with this lazer focused goal, Tenable has developed a suite of product and solutions to audit and mitigate the potential weakpoints of your digital infrastructure. As a trusted partner, we have access to tools and analysts that can help you protect your business data.

RJ2 SPOTLIGHT

Jeff Lucius

Senior Project Engineer

Jeff has over 10 years' experience with various technical implementations, management, and administration of small to the Enterprise Level corporations. As part of the Project Management team, Jeff oversees many IT and Consulting engagements for RJ2 Technologies' clients.

Prior to RJ2 Technologies, Jeff was the Technical manager for a large Network Operations Center corporation and was recognized for his leadership during a complex overhaul of system-wide monitoring and remediation of several existing virtual environments. Jeff enjoys spending time with his family.

BUSINESS PRESENCE

Stay afloat during the pandemic: 5 useful tips!

As the coronavirus disease continues to spread all over the world, more and more businesses are faced with a difficult decision: find a way to adapt to the current situation or close their doors forever. Here are some tips to help your business adjust to the challenges of the pandemic and stay afloat during these tough times.

Reduce expenses

Putting off non-essential or discretionary expenses, such as repainting your offices or buying new equipment, is a no-brainer. Cutting out fixed expenses such as rent and loan payments is harder, if not impossible, to do. However, it is crucial if your production and revenue are at a standstill.

Learn from your competitors

Observe both your direct and indirect competitors, especially those that are faring better than others. Find out what they're doing differently and see if this will work for your business. More than adopting these strategies, it's important to adapt them to your own and your customers' needs.

It's also a good idea to look at larger organizations within your industry. SMBs like yours may not be able to compete with bigger players on a scale level, but you can learn a few things about customer service, marketing strategies, and the like from them.

Redefine your business model

Even with coronavirus restrictions gradually being lifted across the United States, it would take a while before things return to normal. It's crucial to ask yourself if traditional business models would still make sense in a post-COVID-19 world and adjust accordingly.

Determine any changes you need to make to your current business model. This involves identifying who your customers are and what they need, your staff's capabilities, and any uncertainties and their impacts.

Connect with your customers

Keeping your customers informed throughout these trying times is important. Make sure, though, that what you're saying is relevant to them. For example, if you run an eCommerce business, let your customers know through email or social media about any shortages in supply and when you expect to be able to fulfill their orders. Doing so reassures customers that you're doing your best to provide them with the same quality of service pre-COVID-19.

Upskill your staff

Upskilling your employees may be the best way to spend your resources during the current situation. Equipping your team with new knowledge and skills will help them adapt to the changing business environment.

Sharpening your team's digital skills is especially important now that the COVID-19 crisis is spurring digital transformation. Other areas to focus on are project management, communication, data analytics, and digital marketing. And if you find yourself short-staffed, it might pay to train employees to handle other aspects of your business, ensuring that everything runs smoothly throughout the pandemic and beyond.

Feature Partner Product: Tenable.sc

Get a risk-based view of your IT, security and compliance posture so you can quickly identify, investigate and prioritize vulnerabilities.

Managed on-premises and powered by Nessus technology, Tenable.sc provides the industry's most comprehensive vulnerability coverage with real-time continuous assessment of your network. It's your complete end-to-end vulnerability management solution:

- Discover: Active scanning, agents, passive monitoring and CMDB integrations provide a complete and continuous view of all of your assets—both known and previously unknown.
- Assess: With coverage for more than 56,000 vulnerabilities, Tenable has the industry's most extensive CVE coverage and security configuration support to help you understand your security and compliance posture with confidence.
- Prioritize: Tenable's Predictive Prioritization technology combines vulnerability data, threat intelligence and data science to give you an easy-to-understand risk score so you know which vulnerabilities to fix first.

Call RJ2 to learn more about your Cyber Exposure Score Today!

June

" Technology is best when it brings people together."
- Matt Mullenweg

TIP OF THE MONTH

Tips to Save You Time!

1. **Search Google with a Right-Click**
2. **Password Managers can log in for you**
3. **Create Templates for frequently used documents**
4. **Get a second monitor**
5. **Use F5 to refresh a brower webpage**
6. **Use a dailer to help make more calls**