frogworks

January 2026

Issue 01 Volume 16

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Businesses Paying Ransom Still Lose Their Data

Few things cause a business owner to panic like ransomware. And when systems freeze, files lock, and the business grinds to a halt, paying the ransom feels like the only way out. But new research shows that paying up doesn't guarantee anything, especially not the safe return of your data.

According to a 2024 survey from Veeam, ransomware data loss is worse than ever. Only one in three businesses (32%) that paid the ransom actually got their data back last year, compared with more than half (54%) in 2023. That's a sobering drop, and a clear sign that cybercriminals are no longer keeping their end of the bargain.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Businesses Paying Ransom Still Lose Their Data

Paying the Ransom Doesn't Pay Off

For years, the business model for relying on ransom payments was straightforward: They'd encrypt your files, demand a fee, and (supposedly) hand over the decryption key once you met their payment demands.

But today's reality looks much bleaker. Now, business owners commonly find that their data remains locked or corrupted even after making hefty ransom payments. Some attackers take the money and disappear, while others send faulty keys that fail to decrypt files. The result? Ransomware-related data loss and expensive downtime that incapacitate operations for weeks.

Paying the ransom can make you an easy mark for attacks in the future. Cybercriminals share information about companies that are willing to pay, putting you on a virtual target list.

More Companies Are Fighting Back

Despite the likelihood of permanent data loss to ransomware, the same Veeam report also found that the number of organizations recovering their data without paying ransom more than doubled between 2023 and 2024. Today, 30% of organizations that fall victim to ransomware attacks don't hand over a dime but still retain their data.

Businesses are becoming more savvy about data recovery and cybersecurity breaches. They're investing in immutable backups (copies that can't be altered or deleted), cloud redundancy, and recovery plans that keep operations moving even during a cyberattack. Instead of surrendering to criminals, they're regaining control and protecting themselves from the financial and reputational damage that comes with ransom payments.

Still, every locked server, encrypted file, and delayed project adds up to lost productivity, shaken client trust, and long-term financial strain. For many small- to mid-size businesses, the cost of business disruption far exceeds the ransom itself.

Protect Your Business Before It's Too Late

Every business is a potential target, and it's impossible to prevent every attack. However, companies minimize the fallout when hackers successfully steal your encrypted files.

The smartest defense is preparation. Begin by auditing your backup systems to guarantee that copies of important data are stored securely and offline. Train employees to recognize phishing attempts and regularly test your data recovery process so you're not caught off guard when a real incident happens.

Refusing to play by the attackers' rules will also help keep your company on track. Understand that paying the ransom doesn't mean getting your data back. Investing in proactive cybersecurity and reliable data recovery strategies is the most effective way to protect your business from ransomware, data loss, and costly disruptions.

New Phishing Kit Turns PDFs Into Malware Traps

Cybercriminals have a new tool to exploit businesses by tricking them into revealing sensitive information. Unfortunately, this one targets a trusted file type that most of us use daily: PDFs.

Security researchers at Varonis recently discovered a dark web tool called MatrixPDF. This PDF phishing malware kit makes it disturbingly easy to turn ordinary-looking PDF files into phishing traps.

Sellers claim that this tool is a legitimate "training" tool for cybersecurity awareness programs. It's not. It's actually a malicious PDF phishing attack that makes it easier for hackers to steal from unsuspecting businesses.

What the MatrixPDF Phishing Toolkit Can Do

Cybercriminals are promoting MatrixPDF: Document Builder - Advanced PDF Phishing with JavaScript Actions as a training tool for crafting realistic simulation PDFs. In plain English, it allows attackers to create fake documents, such as invoices or contracts, that appear completely legitimate but contain hidden scripts. These hidden scripts can trick users into giving up login credentials, financial information, or access to company systems.

This PDF to malware phishing kit stands out because it offers:

- A simple interface, so even amateur criminals can use it
- Convincing fake documents
- A lower price than similar tools on the dark web

In short, it makes it much easier for low-skill hackers to launch sophisticated attacks.

New Phishing Kit Turns PDFs Into Malware Traps

Why You Need To Be Concerned

PDFs are everywhere in business. We trust them and usually open them without a second thought. This practice makes the new PDF phishing malware kit even more dangerous.

MatrixPDF documents are incredibly realistic-looking, so spotting them is no longer just about spotting bad grammar or misspellings. These fake PDFs blend in seamlessly with everyday business communication, and your employees won't catch them by looking for typos.

The developers also included tools that help ensure these harmful documents actually land in inboxes. They baked in protections like secure redirects, encrypted metadata, and content blur so they can sneak past email security tools.

How To Protect Against PDF Malware Traps

MatrixPDF might sound frightening, but you aren't helpless. Knowing how to detect malicious PDF phishing attempts can save your company from a costly breach.

Other practical steps that can make a real difference include:

- Train your team to verify senders before opening attachments, especially PDFs from unexpected sources
- Keep your PDF readers, browsers, and security software updated
- Consider email security tools that can scan for malicious scripts hidden in attachments
- Create a culture where employees automatically ask, "Does this look right?" before clicking

The new MatrixPDF phishing toolkit is a wake-up call for business owners. With criminals selling advanced tools that turn PDFs into weapons, it's more important than ever to strengthen your defenses.

Don't Fall Into the Trap

Tools like MatrixPDF are here to stay. As long as there's money to be made from cybercrime, criminals will continue to develop PDF phishing malware kits and easier, cheaper ways to attack businesses.

The good news? Most successful attacks rely on people not paying attention. Train your team, keep your software current, and treat PDFs from unknown sources with the same skepticism you'd give a suspicious link. Then, your company won't be an easy target.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter