frogworks

December 2025

Issue 12 Volume 15

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Microsoft Word just made losing files much harder

Have you ever lost an important document at the most inopportune moment? It's frustrating and can cost your establishment time, money, and trust.

The latest Microsoft Word file recovery feature makes it easier than ever to retrieve unsaved or lost contracts, reports, project plans, and more. Learn more about it here.

What Is a Cloud Storage Backup?

As the name suggests, it's a system that stores your files in the "cloud" or remote online servers. Microsoft has revealed plans to automatically save all Word documents to OneDrive, the company's own cloud storage service.

At some point during our daily operations, we've all wasted minutes, sometimes hours of work, because we forgot to hit save after working on a document.

With this key change, you no longer need to initiate the first save manually. The cloud copies new documents automatically by default before you even assign a file name. It's especially helpful for hybrid, remote, or on-the-go work setups where cross-device syncing is a necessity.

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

Microsoft Word just made losing files much harder

How Business Owners Can Enable Automatic File Saving

The Microsoft Word file recovery feature is currently only available to Microsoft 365 Insiders; however, it is expected to expand to all users in the future. If you have a Microsoft 365 Personal, Family, or Business (for administrators only) subscription, you're eligible to join the Insider program.

Members get two options: the Beta Channel and the Current Channel (Preview). The former works best for anyone who wants to use the latest unsupported builds to help identify issues and offer feedback on new features. The Current Channel is the preferred choice if you want early access to features and enjoy stable updates.

Balancing Convenience and Security in OneDrive Integration

Anyone with your credentials can access all files saved to OneDrive, so you need to enforce strong passwords, two-factor authentication, and strict, regularly audited access permissions.

When data breaches occur or login details get stolen, having a backup plan is crucial. Utilize data protection options, such as document recovery tools, and regularly update credentials. Monitor unusual account activity closely.

Some users are also concerned that this feature is simply Microsoft's strategy to sell more cloud storage. When it finally becomes the default setting, you can opt out by going to the Save page of Word Options and deselecting "Create new files in the cloud automatically."

Modern Tools To Make File Management Easy

The latest Microsoft Word file recovery tool may seem unnecessary, especially with version history and autosave options already built into the software. For those who occasionally forget to hit save or encounter crashes, however, having an extra safety net could become a lifesaver.

Buy Those Christmas Gifts!

Interlock Ransomware Is Escalating, So Protect Your Systems Now

In the ever-evolving world of cybercrime, one name has rapidly climbed the ranks: Interlock Ransomware. Typically brushed off as just another mid-tier credential stealer, Interlock has morphed into something far more dangerous.

Cybersecurity firm Forescout reports that this threat actor has officially entered the "operational maturity" phase, meaning it can now successfully target high-value industries like healthcare, government, and manufacturing.

That doesn't mean that small and mid-size businesses aren't still at risk, though.

The Evolution of Interlock Ransomware

At its earliest appearance in mid-2024, Interlock Ransomware primarily targeted the theft of credentials, such as passwords and access tokens, as well as other sensitive data. But Forescout's latest report reveals that by February 2025, Interlock had become a fully-fledged ransomware enterprise.

This new phase means Interlock can launch ransomware attacks at scale, encrypting data across networks, cloud environments, and devices with frightening precision. It's also developed beyond simple malware into a cloud-enabled, multi-platform operation. Think of it as organized crime with a tech startup's polish, thanks to its professional affiliates, automated attack tools, and even "support channels" for victims who pay ransoms.

How Interlock Ransomware Operates

Interlock takes a sophisticated approach to its attacks. The malware relies on automated lateral movement within networks to search for valuable files. Once it locates what it's searching for, it deploys data encryption payloads.

However, once it's inside a system, it can:

- Exfiltrate sensitive information before locking files, allowing double extortion
- Spread to additional networks through phishing emails and compromised software updates
- Deploy payloads on both Windows and Linux environments, increasing its reach.

The result? A single compromised employee email could cause a full-scale network lockdown and a ransom note demanding payment in cryptocurrency.

Interlock Ransomware Is Escalating, So Protect Your Systems Now

Your Business Is at Risk

Interlock's use of automation and cloud-based command centers allows it to target smaller organizations, too. Your small business is just as much at risk as a major corporation.

And Interlock's affiliate program—a network of independent hackers who rent its ransomware tools—means attacks can happen anywhere, anytime. That makes cybersecurity measures and threat mitigation strategies more critical than ever.

Taking steps to reduce the attack service and catch signs of the malware early can help you get (and stay) ahead of the threat.

- Educate your team: Ransomware attacks often begin with phishing, so provide regular training to employees to spot suspicious links and attachments.
- Keep backups secure: Store data backups offline or in isolated environments to enable quick recovery.
- Update and patch software: Outdated systems are prime entry points for attackers.
- Segment your network: Limit how far ransomware can spread if it gets in, and watch for lateral movement throughout the network.
- Watch for unusual activity: Use behavioral analysis to identify possible infiltration and anomalies in authentication logs.
- Implement strict risk-based, conditional access controls: If someone doesn't need access to a network segment, they shouldn't have it.

Don't Wait for a Wake-Up Call

Interlock Ransomware is a wake-up call for every business owner who wants to avoid the financial, reputational, and operational costs of a ransomware attack. If you haven't reviewed your network defense or backup strategy recently, now's the time. Prevention can ensure your company's survival.

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