RANSOMWARE ON THE RISE

A deeper look at one of the top cybersecurity threats in 2023

Insight

Evolving ransomware: What you need to know

Because of its low cost and high profit model, ransomware remains one of the largest cybersecurity threats on the web today. In fact, the 2022 Mid-Year Cyberthreat Report by Acronis[1] called ransomware the number-one threat to large and medium-sized businesses.

Ransomware is a form of malicious software designed to encrypt files and render systems and data unusable until a ransom is paid.

Global ransomware damages are estimated to exceed **$30 billion** by 2023.[2]

In August of 2021, IDC reported that more than **one third of organizations experienced a ransomware attack** in the last 12 months.[3]

623 million:
The ransomware attack volume in 2021 — **105% higher** than 2020's total.[4]

The preferred delivery method of ransomware attacks? Phishing and malicious emails.

Unfortunately, modern phishing attempts are becoming more and more difficult to spot. Even with security training, many employees struggle to recognize a phishing attempt. It's vital that businesses safeguard their systems and data.

Why has ransomware become so prominent?

Profiting from ransomware is a simple, lucrative method of attack for cybercriminals. Many major attacks are run by organized ransomware gangs attempting to gain acceptance as legitimate enterprises.

According to the October 2021 Microsoft Digital Defense Report, the publicly reported profits from ransomware and extortion attacks give attackers a budget that would likely rival that of nation-state attack organizations.[5]

In June of 2021, Reuters reported that the U.S. Department of Justice elevated investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack.[6]

Having preventative and protective measures in place is vital for every business. Keep reading to learn more about ransomware, phishing and powerful security tools.

Phishing prevention

We know phishing is a favorite method of ransomware delivery, but how do hackers implement these attacks? Phishing relies on human error by manipulating users into providing sensitive information to cybercriminals.

For instance, a malicious email masked as a company communication may include dangerous false links. With just one click, an employee can unknowingly expose your business, team and sensitive data.

Staff training is critical in this area, but as attacks become more sophisticated, malicious emails are harder to identify. That’s where preventative software comes in.

Email security software delivers a robust defense against malicious messages. With tools such as firewalls, encryption and filtering, it’s harder for bad actors to enter your internal systems. Proper email security can mitigate the risk of phishing attempts, viruses, malware and spam messages.

It’s time to implement robust cybersecurity.

When it comes to ransomware, prevention is key. Do you have the right systems in place? Ensure that your business has these measures in place:

- Regular system updates
- Restricted permissions and limited network access
- Advanced email phishing protection
- Automated, secure data backup tools
- Strong Identity and Access Management (IAM) security

Additional tools can minimize your vulnerability as well. Strong endpoint security can keep employee devices safe from attempted malware, and modern endpoint tools evolve and expand to meet the increasing number and variety of devices across your network.

Application and cloud security are also vital in today’s workforce structure. Powerful post-deployment application protection will minimize the risk of threats, breaches and code hijacking, while cloud defense enables your enterprise to modernize and scale with confidence.

Defend the backbone of your business.

Your business relies on the constant flow of data. Trusted tools for encryption, access and tokenization will support your security efforts. At Insight, we have a deep catalog of encryption and data management tools to defend your most valuable information — while it's stored and while it's in transit.

Data privacy laws are constantly evolving, and our experts will keep your assets protected, compliant and secure with customized defense.

With the right data protection, you'll bolster your regulatory reputation and financial health.

A partner you can trust

Defending your business against ransomware is an ongoing task, and taking this on without an experienced partner can lead to a host of challenges. Luckily, Insight experts can guide you from end to end, offering improved efficiency, enhancement and strategic alignment.

With Insight on your side, you'll unlock:

- Optimized costs
- Improved accuracy for entitlement
- Better forecasting for future needs
- Increased readiness for internal and external audits
- A modernized data center with comprehensive protection
- Consistent compliance

Set the security standard.

Shield against sophisticated attacks with leading cybersecurity. Talk with an Insight expert to find the right technology for your team.

About Insight

Insight Enterprises, Inc. is a Fortune 500 solutions integrator helping organizations accelerate their digital journey to modernize their business and maximize the value of technology. Insight's technical expertise spans cloud and edge-based transformation solutions, with global scale and optimization built on 34 years of deep partnerships with the world's leading and emerging technology providers.

Insight®

1.800.INSIGHT | insight.com

[1] Acronis. (2022). Acronis Cyberthreats Report Mid-year 2022.

[2] Acronis. (2022). Acronis Cyber Protection Operation Centers Report: Ransomware dominates threat landscape.

[3] Dickson, F. Kissel, C. (July 2021). IDC's 2021 Ransomware Study: Where You Are Matters! IDC.

[4] SonicWall (2022). 2022 SonicWall Cyber Threat Report: Cyber Threat Intelligence for Navigating The Unknowns of Tomorrow.

[5] Microsoft. (Oct. 2021). Microsoft Digital Defense Report.

[6] Bing, C. (2021, June 3). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. Reuters.