Ransomware attacks have increased by 50% in Q2 2019

Ransomware is evolving at a rapid pace. Ransomware attackers implement new techniques that evade and bypass traditional defenses. As a result, businesses end up paying ransoms rather than lose access to their intellectual property, credit card information, patient records, and other business data.

Do you know your enemy?

Ransomware attacks users in multiple ways, encrypts and holds your data for ransom (usually cryptocurrency). Many times, data is not released even after the ransom is paid. You could be vulnerable to ransomware attacks if you:

- Use a legacy software
- Use an unpatched vulnerable browser or operating system; Windows 7 is twice as likely to be hit than Windows 10
- Don't have a reliable back up plan
- Lack comprehensive cybersecurity strategy

Losses due to Ransomware are predicted to reach $20 Billion by 2021[1]

Ransomware attacks business every 14 seconds[2]

Ransomware attacks are growing at a yearly rate of 350%

How does your business get affected?

69% Phishing

40% Drive by Download

44% Malicious Click

42% Botnet

1 & 2: Cybersecurity Ventures

Trigent Software, Inc. ■ 2 Willow Street, Suite 201, Southborough, MA 01745 ■ +1.508.779.6743 ■ www.trigent.com

TRIGENT
OVERCOMING LIMITS

How ransomware works?

Multiple attack methods
Ransomware can attack through many ways - emails, targeted spear phishing, malicious websites, etc.

Malware Execution
Script is executed as the malware gets installed in the operating system.

File Encryption
The ransomware code encrypts the data on the system.

Ransom Demand
The attacker demands the cryptocurrency to decrypt the data.

Make sure you are not a victim

Proactive measures to keep ransomware out of your business.

- **Backup:** Ensure you always backup your data, both locally and offsite. Follow 3-2-1 mantra. 3 Copies; 2 different media; 1 offsite.
- **Segment network access:** Segregate your network into distinct zones, each requiring different credentials.
- **Early Threat Detection Systems:** Early unified threat management programs can find intrusions as they happen and prevent them.
- **Invest in layered security:** Installing multiple layers of cybersecurity protection - firewall, anti-malware/ransomware, and anti-exploit technology.
- **Run frequently scheduled security scans:** Run scans on your computers and mobile devices regularly; they form the second layer of defense in the security software.
- **Update software and apply patches:** Install the latest updates and patches on your computers and mobile devices.
- **Educate and train users:** Educate your users to recognize phishing campaigns, suspicious websites, and other scams.

Achieve ransomware resilience with Trigent

Ransomware is like the elephant in the room that only gets bigger. To fight against ransomware, you require a risk management strategy that is beyond data security. Trigent can help deliver the most effective ransomware mitigation and business continuity solution. We offer superior backup solutions both on-premises and cloud, whether you are restoring an entire server or specific files to restore. Our services provide:

- DNS Level Security
- Anti-Malware Security
- Network Segmentation
- Visibility Enforcement
- Email and Web Security
- Infrastructure segmentation and intrusion prevention
- Incident Response and Management

Need help with protecting your business from ransomware attack?
Call us at **+1.508.779.6743** or email us as **sales@trigent.com**

TRIGENT
OVERCOMING LIMITS