Fight Double Extortion Ransomware Threat with Essential Security

Late in 2019, a new cyber security threat emerged. Criminals used ransomware to attack Allied Universal. In a twist now known as double extortion, the bad actors first extracted sensitive information before encrypting company data. Then they insisted that Allied pay a stiff ransom to avoid seeing sensitive data leaked publicly.

Throughout 2020, other attackers have followed suit. To convince organizations to pay a ransom, criminals threaten to publish or sell the stolen data. To prove their point, they post samples of the data on their websites. Thus, the tactic effectively combines ransomware with data breach. And it places organizations in an extremely difficult position.

Understand the Process

To effectively counter the threat of double extortion, organizations must understand the process and the dangers. First, attackers infiltrate and infect the system. Often, they use phishing emails as a vehicle. Additionally, the COVID pandemic opened vulnerabilities as companies rushed to accommodate remote workers, leaving security gaps.

Next, attackers extract a copy of sensitive information for themselves and then execute the ransomware, locking users out of their own data by encrypting it. Most often, all of this occurs before the organization realizes it has an intruder in the system.

Finally, the victim receives notification of the attack, along with a ransom demand. To pressure the victim to pay the ransom, the attacker may publish bits of the stolen data online. As the days pass, the ransom demanded increases. And if the organization still refuses to pay, the attackers publish or auction off all the data.

As a result, the costs mount up quickly. Remediation after an attack can cost more than the ransom itself. And a data breach often means the organization must report to the appropriate data privacy agency, incurring both stiff fines and reputation loss.

Steps to Prevent a Double Extortion Attack

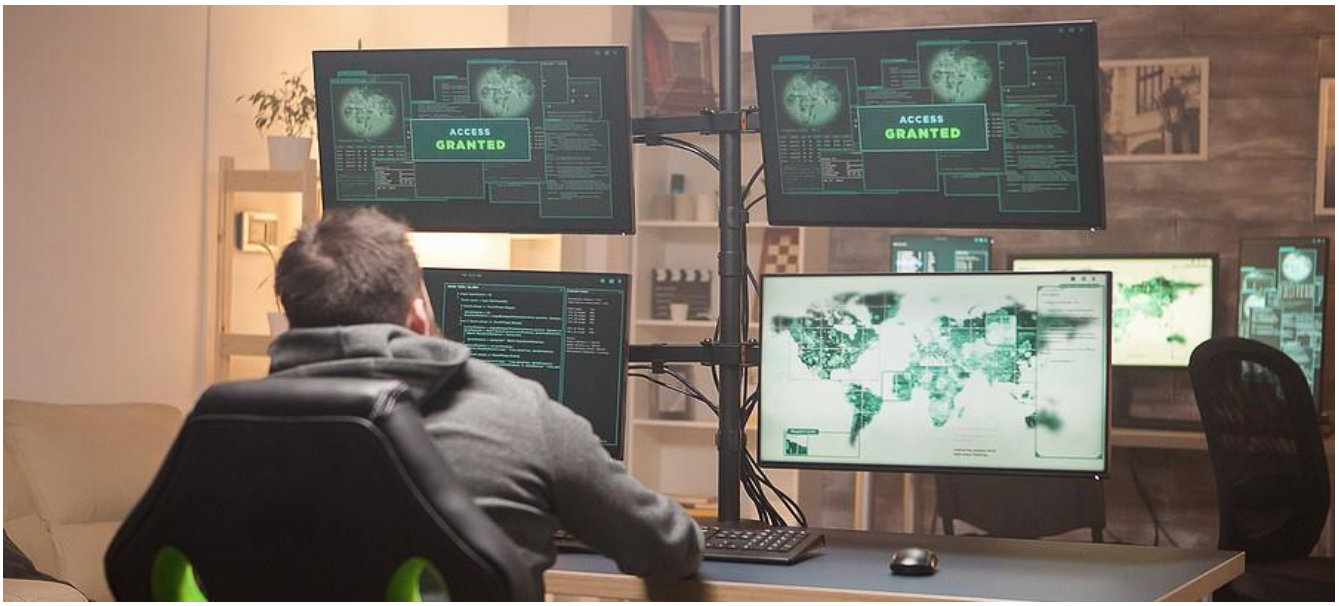
While no organization can assume it will remain safe from ransomware, the following practices, when combined, offer essential first steps.

- **Timely updates** – Be sure to apply security updates to hardware and software in a timely fashion. This includes anti-virus and anti-malware.
- **Access management** – Enforce effective password policies and incorporate multi-factor authentication where possible. Additionally, limit user access to only those functions and areas of the system the users need to complete their work.
- **Endpoint security** – As the COVID pandemic got underway, organizations needed to accommodate remote work literally overnight, sometimes leaving systems vulnerable. Implement solid endpoint security to reduce the attack surface.
- **User education** – Cyber criminals continue to focus on the weakest link in our security strategies by targeting end users. Teach employees to practice safe computing through regular, focused cyber security training.

Strategies to Minimize the Effects of an Attack

A recent study estimates that cyber criminals attack a business every eleven seconds, using increasingly sophisticated methods. Consequently, organizations need to combine prevention with efforts to limit the damage caused once an attack occurs. The following strategies will help.

- **Network monitoring** – Attackers can spend weeks or even months lurking in your network. To protect your organization, you need to find and contain the infection quickly to minimize the damage. To that end, employ 24/7 network monitoring to uncover any anomalies that might indicate a breach.
- **Encryption** – By encrypting sensitive files within your system, you deny cyber criminals the ability to sell or publish company data. This protects your organization from data breach and reduces the attacker's bargaining power.
- **Backups** – Backups will not save compromised data in a double extortion scheme. However, if you can protect sensitive data from breach with encryption, backups will prove essential in recovering from ransomware.
- **Disaster recovery plan** – Be sure to have a plan in place in case an attack occurs. This should include communication procedures, as well as a prioritized list of data sets to recover.



Counter Threats with Comprehensive Security

As cyber threats continue to evolve, cyber security strategies must evolve at pace. eMazzanti provides the tools and expertise you need to both prevent attacks and minimize the damage when attacks do occur.

For instance, our network services can identify potential threats before they compromise your system. We also offer remote workforce security, email protection, dark web scanning and more. We will customize a security solution geared toward your specific business needs and budget.