Quantum Ransomware Strikes Quickly, How to Prepare and Recover

The business world recently received yet another cyber security wakeup call in the form of the Quantum ransomware attack. In one of the fastest ransomware attacks yet reported, attackers moved from initial attack to ransomware deployment in under four hours. Understanding attack patterns can help organizations mount more effective cyber defenses.

Familiar Ransomware Rebranded…With a Twist

While Quantum has made headlines in recent days, the ransomware actually surfaced two years ago. Known initially as MountLocker, it was rebranded as Quantum in August 2021 when the encryptor began adding .quantum file extensions. Like other ransomware operations, it takes over networks, compromising servers, encrypting files, and bringing work to a halt.

The speed of attack makes these recent ransomware events particularly concerning, especially as it signals a growing trend. Four hours to complete domain takeover gives organizations very little time to mount an effective defense.

Anatomy of a Typical Quantum Ransomware Attack

While Quantum attacks leave scant time to react, knowing how typical attacks occur helps organizations with both prevention and mitigation. For instance, in recent Quantum ransomware attacks, infection occurred through a phishing email. While seemingly from a legitimate source, the email included IcedID malware embedded into an attached ISO file.

Once the unsuspecting user clicked the attachment and executed the malware, threat actors were able to compromise a server on the network, installing Cobalt Strike. While initially developed for legitimate penetration testing, bad actors use this utility to dive deep into victim systems.

For instance, by deploying Cobalt Strike they mapped out the network structure and extracted admin credentials. Armed with that information, they then connected to other servers in the network and deployed ransomware throughout the system.

Strategies for Preventing and Detecting Attacks

Because the Quantum attacks happen so quickly, organizations must use a multi-layered approach to defense. For instance:

- Implement 24/7 security monitoring – Successful defense depends on catching suspicious activity immediately. Implement continuous, automated monitoring to identify anomalies and take appropriate action.
- Update email filtering – Email represents the most common attack method. A comprehensive email filter will scan for phishing and malware and block certain types of attachments.

- Turn on multi-factor authentication (MFA) – Security experts emphasize the importance of turning on MFA for all systems that allow remote connections. This key step helps stop bad actors from connecting remotely from one server to another to spread ransomware.
- Train end users… again – No technology solution can guarantee full security. A comprehensive strategy must include regular security awareness training for all end users. Focused, engaging, repeated training will help users spot and avoid potential phishing situations.

Quantum Ransomware Recovery Tips

If the worst happens, and your organization gets hit by Quantum or another ransomware, have a recovery plan in place. A well-documented incident response plan saves precious time and provides a much greater chance of successful recovery. The recovery plan should include key team members, communication plans and steps for malware containment and eradication.

Another critical component of a recovery plan involves data backups. Without solid backups, organizations may have to choose between losing critical data and cooperating with threat actors. Implement automated backups, test them regularly and store a copy offline to keep it safe from attack.

Additionally, be sure to involve the right players. Partner with security personnel who are well-versed in ransomware recovery and have the right tools at hand. You may also need to involve the FBI, cyber breach lawyers, communications personnel, and your insurance provider.

The cyber security experts at eMazzanti provide the tools and experience you need to implement a comprehensive security strategy. From monitoring to email filtering and end user training, we will help you stop malware earlier and recover quickly in the event of infection.