What You Need to Know About Ransomware

What is Ransomware?

Ransomware is a type of malicious software, or malware, that blocks access to a system, device, or file until a ransom is paid. It is an illegal, moneymaking scheme that can be installed through deceptive links in an email message, instant message, or website. Ransomware works by encrypting files on the infected system (crypto ransomware), threatening to erase files (wiper ransomware), or blocking system access (locker ransomware) for the victim.

The ransom amount and contact information for the cyber threat actor (CTA) is typically included in a ransom note that appears on the victim's screen after their files are locked or encrypted. Sometimes the CTA only includes contact information in the note and will likely attempt to negotiate the ransom amount once they are contacted. The ransom demand is usually in the form of cryptocurrency, such as Bitcoin, and can range from as little as several hundred dollars up to and exceeding one million dollars. It is not uncharacteristic to see multi-million-dollar ransom demands in the current threat landscape.

What Can You Do About Ransomware?

Defending against ransomware requires a holistic, all-hands-on-deck approach that brings together your entire organization. While ransomware infections are not entirely preventable due to the effectiveness of well-crafted phishing emails and drive-by downloads from otherwise legitimate sites, organizations can significantly reduce the risk of ransomware by implementing cybersecurity policies and procedures and improving cybersecurity awareness and practices of all employees. It is up to all of us to help prevent ransomware from successfully infecting our systems.

To increase the likelihood of preventing ransomware infections, organizations must implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. This program should include organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.

This is why we do what we do at Milima Security through our study courses at Milima Cyber Academy. Click here to find out more about our courses.