RANSOMWARE Q&A

ROB BENNETT, LIGHTEDGE SECURITY MANAGER

LIGHTEDGE

WHY ARE WE SEEING AN INCREASE IN RANSOMWARE?

RB: Although there are a wide variety of complex answers to this question, I look at this answer as having five key points:

◢ Threat actors understand organizations have a difficult time with cyber hygiene, which includes properly deploying patches and addressing vulnerabilities patching does not resolve. This is a crucial step in stopping these exploits as they almost always use known vulnerability to exploit.

◢ Organizations often leave services open to the public Internet unnecessarily. If your organization is a LightEdge customer, we can assist you in detecting these exploitable openings.

◢ Humans are curious, which can be both a blessing and a curse. Have you ever received an email with a catchy subject line and immediately sucked in? When these emails contain a link, do not open it. This is the easiest way for threat actors to gain access to your system. Contact your Security Team if you are unsure if the email originated from a trusted source. It may sound simple, but with phishing on the rise, taking these small steps may save you from disaster.

◢ Employees reuse passwords frequently across various systems. There have been countless breaches caused by an employee using the same password across all their systems and their personal accounts. Requiring different usernames and passwords for work and personal accounts is critical for your organization's security as well as the security of your employees' personal information.

◢ The hard truth is that many organizations have either over-spent on tools that are not monitored by trained professionals or they have not spent enough on the tools to identify and raise the alarm in the event of an intrusion. Something as easy as your organization anti-virus sending an alert after hours or on weekends to notify a trained team member of the alert when it occurs.

WHAT MAKES THESE ATTACKS SO SUCCESSFUL?

RB: There are two reason that stand out. The first is that there are not enough trained IT staff members who are equipped to take on these challenges when an attack occurs. I highly recommend the tabletop exercises provided by the FBI and CISA, along with exercises that should be included in your organization's cyber insurance policy.

Additionally, employees do not receive enough security awareness training on how to spot phishing attempts or what to do during a ransomware event. This can cause them to miss critical steps to containing it. For example, someone's first instinct might be to shut down your systems. Although this might be a decent response, there are often several other steps that need to be completed in order to oust the threat actor from your system.

WHAT IS THE MOST DANGEROUS RANSOMWARE ATTACK?

RB: It's pretty hard to rank the danger level of a ransomware attack because it all depends on the duration of the attack and how long it takes an organization to notice something is amiss. Each threat actor has their own methods to exploit and exfiltrate your data.

The newest versions of Egregor exploit open, unpatched RDP sessions and phishing campaigns are threats businesses should be mindful of if their organization utilizes RDP extensively. Conti is another threat that utilizes multiple attack vectors, leaves backdoors, and utilizes legitimate memory resident security tools. Finally, malware threats often need to be discovered, remediated, and validated before a business confidently say their organization is clean.

WHAT ARE SOME BEST PRACTICES I CAN START UTILIZING RIGHT AWAY TO PROTECT MYSELF AND MY ORGANIZATION FROM A RANSOMWARE ATTACK?

RB: Overall, I recommend having good cyber hygiene practices, including any and all of the following:

- Patch your endpoints
  - Monthly cycle for Microsoft and Apple systems
  - Quarterly cycle for other systems
- Regular scans to ensure the organization does not leave systems exposed
- Restrict user access
- Remove local admin privileges on user endpoints and limit domain admin memberships
- Email scanning to catch known threat campaigns
- Place a banner on all emails you receive from outside parties to help identify possible threats
- Firewalls
  - Geo-Block countries you do not do business in
  - Implement web filtering to block known malware and other nefarious sites
  - Annual Reviews of your firewall to ensure the configuration is following best practices
- Awareness training for staff
- Monitor your business processes and know the purpose so you can detect abuse
- Ensure backups are maintained, restorable, and archived off site
- Implement Multi-Factor Authentication for access to the network and email at minimum

By utilizing even a few of these best practices on the list above, you can begin to set your organization up for cybersecurity success. It's always better to do something than nothing.

WHAT DOES THE FUTURE LOOK LIKE FOR RANSOMWARE?

RB: While we don't have a crystal ball, I can confidently say that until attack methods stop making revenue, they will still be used by threat actors. Threat groups are more similar to a legitimate business venture than you think, as they essentially behave like a corporation. They have revenue goals, specialized teams to exploit an organization, and they share effective attack techniques and valuable intel across organizations. Unfortunately, cybercriminals are currently winning the cyberwar and everyone from the bottom up in your organization needs to understand effective prevention methods, as one wrong click could damage your companies reputation to customers, employees and business partners.

EXPECT TOP-NOTCH RANSOMWARE PROTECTION WITH LIGHTEDGE

Ransomware attacks continue to grow in frequency and complexity. LightEdge constantly renews its promise to take a proactive stance when delivering top network safeguards. Our network is intentionally built to handle mission-critical, compliant workloads with the highest standard or security in mind. We also recommend layering on our DDoS Protection services for the fastest possible threat detection and downtime mitigation before disaster ever strikes.

We understand it may be too late in some instances and you may already be reactively operating in emergency mode. If your company is currently under attack, LightEdge can step in and work with you to figure out a solution. If you're concerned or experiencing issues, contact us immediately at 1.877.771.3343.