PUBLICATION

Beware of Cyber Attacks During the Holiday Season – Royal Ransomware Group Highlighted as Threats to the Health and Public Health Sectors

Authors: Layna S. Cook Rush
December 21, 2022

Statistics show that cybercrime increases significantly during the holiday season. Threat actors anticipate that workers are distracted and more likely to fall victim to a phishing email scam than any other time of the year. Many employees are out of the office during the holiday season, including IT staff. This means that cyber-attacks are more likely to be undetected and response time by an organization is slower. Additionally, most organizations indicated that they would lose more money if a ransomware attack occurred over a holiday. A recent survey of more than 1,200 cybersecurity professionals indicated that over 33 percent of businesses said it would take their organization longer to assess and respond to a cyber-attack over a holiday than at other times.

Ransomware groups, in particular, are keen to strike during the holiday season. Last year, DarkSide struck Colonial Pipeline Company on Mother's Day; REvil struck JBS Foods on Memorial Day; and REvil struck IT management company Kaseya over the Fourth of July. This year, there is no sign that the ransomware threat is going anywhere.

Earlier this month, the U.S. Department of Health and Human Services (HHS) issued a warning that attacks using Royal; a new strain of ransomware, were on the rise. Since September, the Royal ransomware group has significantly ramped up their operations. In November, Royal took England's most popular racing circuit, Silverstone Circuit, offline. In December, Royal compromised the Travis Central Appraisal District, a property appraisal service, shutting down the company's email, website, and servers for more than two weeks. Due to historic use of ransomware against the health sector, HHS warned that Royal should be considered a direct threat to the health and public health sectors.

Organizations can guard against attacks during the holidays by educating employees about the increased risks and reminding workers of company policies on cyber hygiene and protocols for reporting suspicious emails or other suspect activity.

Preventative measures include:

- Confirm that all software updates and patches have been applied and Safe Links is enabled for all Microsoft products before IT professionals take time off for the holidays.
- Lockdown privileged accounts.
- Review incident response and contingency plans to verify they are up-to date.
- Include contact information for legal counsel, any cybersecurity vendors on retainer, and insurers or brokers in the response plan.
- Ensure key employees with roles in incident response and/or emergency operations have a copy of the incident response and contingency plans readily accessible during the holidays if a cyber incident occurs. Remember that if an incident does occur, electronic copies of incident response plans and contact information for key stakeholders may not be accessible. Have a paper copy handy.

Baker Donelson is an authorized NetDiligence Breach Coach® and is available to assist our clients should an incident occur. We can be reached via our toll-free incident response hotline, 877.215.6115, which is accessible 24 hours, including holidays.

If you have any questions or are interested in learning more about this opportunity, please contact Layna Cook Rush, CIPP/US, CIPP/C or any of our Data Incident Response team members.