Published on *The National Law Review* https://natlawreview.com

FBI/CISA Alert: Increased Likelihood of Ransomware Attacks Over Labor Day Weekend

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Maya Atrakchi

Watch out! A spike in ransomware attacks may be headed our way over Labor Day weekend. Yesterday, the FBI jointly with the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning to be on high alert for ransomware attacks this weekend, after recent targeted attacks over Mother's Day, Memorial Day and Fourth of July weekends.

"Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of ransomware, as network defenders and IT support of victim organizations are at limited capacity for an extended time", the FBI and CISA noted in their alert.

In May 2021, leading into Mother's Day weekend, malicious cyber attackers deployed the now infamous ransomware attack on Colonial Pipeline, resulting in the Biden Administration issuing a memo specifically addressing critical infrastructure cybersecurity. Shortly after, over Memorial Day weekend, an entity in the food and agricultural sector suffered a similar attack, resulting in a complete shutdown of production. And finally, over July 4th weekend, an entity in the IT sector was hit with an attack affecting hundreds of organizations including multiple managed service providers and their customers. Needless to say, organizations across all sectors should be on high alert heading into Labor Day weekend.

The FBI's Internet Crime Complaint Center (IC3), the go-to-source for cyber incident reporting, has tracked ransomware trends in recent years. In 2020, a record number of complaints (791,790) related to internet crimes were reported to IC3, with reported losses exceeding $4.1 billion. In ransomware specifically, there was a 20% increase during 2020, and a 225% increase in ransomware demands.

The FBI/CISA's joint ransomware warning for Labor Day, provides several suggestions for preventing and responding to an attack. **Here are a few key takeaways**:

- *Make an offline backup of your data.* This includes reviewing your organization's back up schedule to consider the risk of possible disruption during weekends and holidays.
- *Do not click on suspicious links*. Implementing an employee/user training program and phishing exercises can go a long way in warding off an attack.
- *If you use RDP-or other potentially risky services-secure and monitor*. In particular limit access and monitor remote access, and *review review review* your third-party vendor's security policies.
- *Upgrade your OS and Software; scan for vulnerabilities.* Continue to review and upgrade your software, regularly patching and updating for the latest available versions that take into account security vulnerabilities.
- *Use strong passwords*. Consistent password hygiene can make a world of difference. Ensure strong passwords, that are regularly updated and not used across multiple accounts or stored on the system.
- *Use multi-factor authentication*. Where possible, implement multi-factor authentication, particularly for remote/virtual networks.
- *Secure your network (s) and user accounts.* This includes securing home networks of remote workers, and regularly auditing user account logs to ensure legitimacy.
- *Have an incident response plan.* There are several steps an organization can take to build an incident response plan that minimizes the chance and impact of a successful attack. Here are a few.

Organizations may not be able to prevent all attacks, but it is important to remain vigilant and be aware of emerging trends, such as spikes in attacks during the holidays. Increasing awareness among employees to avoid becoming a victim of a phishing attack could be an excellent initial step.

National Law Review, Volume XI, Number 246