CYBEREASON GOVERNMENT INC.

2021 RANSOMWARE HOLIDAY ADVISORY

Leading into the 2021 Labor Day holiday Weekend, in a joint advisory, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) warned businesses about the increase in ransomware impacts on holidays and weekends when offices are closed or companies have skeleton crews working. Many of the most disruptive ransomware attacks in 2021 have occurred over holidays and weekends, when fewer people are around to detect the activity and the IT security team is at home trying to relax with family and friends.

Impactful 2021 Holiday/Weekend Ransomware Attacks

May 2021- **Mother's Day Weekend**- **Colonial Pipeline**

May 2021- **Memorial Day Weekend**- **JBS Foods**

July 2021- **Fourth of July Weekend**- **Kaseya Limited**

Sept 2021- **Labor Day Weekend**- **Howard University**

Saturday, October 9- **Ferrara Candy Company**

Saturday, October 18- **Sinclair Broadcasting**

Saturday, October 23- **Schreiber Foods in Wisconsin**

Cybereason's Global Ransomware Holiday Study Summarizes the Business Impact of Ransomware Attacks on Holidays and Weekends

Following the FBI's and CISA's Labor Day Weekend Advisory, Cybereason conducted a global ransomware study to understand the business impact ransomware attacks are having on companies during holiday periods and weekends. Findings from this research

will help guide defenders to act and organizations to get the processes and tools in place to effectively detect and stop these attacks.

Ransomware attacks are having a negative impact on businesses in the U.S. and around the world. Cybereason published a global research study in June 2021, titled *Ransomware: The True Cost to Business*, which found that ransomware attacks cause organizations a significant loss of revenue, damage to the brand, unplanned workforce reductions and disruption of business operations.

In the latest Cybereason survey of more than 1200 businesses in the U.S. and around the world that had suffered a ransomware attack on a holiday or weekend, **90 percent** of respondents indicate they are concerned about being hit by another ransomware attack this holiday season, yet **24 percent of respondents** have no specific plan in place to address a ransomware attack when they only have skeleton crews working on the holidays and weekends. Many companies also have a false sense of security, **with one-in-five respondents** believing they would never be the target of a ransomware attack.

Surprisingly**, 63 percent of respondents** indicated they believed the ransomware attack was successful because it was carried out by an advanced attacker like those backed by a nation-state, even though ransomware attacks are almost exclusively a cybercriminal tactic. While more and more ransomware attacks are the result of more complex RansomOps ‘big game’ hunting carried out by groups such as REvil and DarkSide, most ransomware attacks are still “spray and pray” where cyber criminals rely on mass email spam campaigns that include tainted attachments or links to malicious websites for infections.

Humans Can be the Weakest Link in the Cybersecurity Ecosystem

With more than 3 million global security staff positions open, with 1 million in the U.S. alone, the cybersecurity industry is suffering from a talent shortage. This is leading to additional stress and longer hours for existing security professionals. In the recent study, **86 percent of respondents** were called into work over a holiday or on the weekend because of a ransomware attack at their company, and have missed time celebrating a holiday or important weekend activity with family and friends. And surprisingly, **70 percent of respondents** admitted to having been intoxicated while responding to a ransomware attack on the weekend or during a holiday, a risk factor for organizations that may not have accounted for by incident response plans.

Remediating the Ransomware Risk and Extracting the Threat Actors from Networks

The Cybereason Holiday Ransomware Advisory was created to increase awareness and offer practical advice and recommendations on how to address the ransomware risk to reduce the likelihood of successful ransomware attacks during the 2021 holiday season.

The Defense Industrial Base and Critical Infrastructure Operators have been in the crosshairs of ransomware gangs throughout 2021. The Defense Industrial Base should deploy EDR on all endpoints, per recommendations laid out in the **White House's Executive Order on Improving the Nation's Cybersecurity.** All agencies except the Department of Defense and all Intelligence Agencies are required to deploy Endpoint Detection and Response (EDR) to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

They should also adopt an operation-centric approach to security. Operation-centric security prevents ransomware by leveraging a sophisticated anti-ransomware platform that uses multiple layers of detection to detect both Indicators of Compromise (IOCs) and Indicators of Behavior (IOBs). These capabilities are essential to detection and stopping a ransomware attack.

Also, critical infrastructure operators are in the crosshairs of ransomware gangs. Operators running outdated and unpatched software are the most vulnerable. Extorting ransoms and testing the resiliency of systems are equally important to threat actors. Causing damage to electricity networks, water systems, SCADA systems, telecommunications systems, aviation systems and rail systems could have long lasting and damaging results.

For critical infrastructure operators to reduce risk, these best practices are recommended:

- **Establish Cyber Incident Response Tools and Procedures Across Both IT and OT Networks with the Goal to Minimize Mean-Time-To-Response:** Minimizing damage and preventing an ICS network from being taken offline is essentially the cat and mouse game being played by attackers and defenders. To keep hacking groups at bay, organizations need to minimize the time it takes to respond to a threat. This can be achieved by deploying threat hunting services around the clock.

- **Establish Unified Security Operation Center and Workflows Across Both IT and OT Environments:**
  Operating a unified security operations center (SOC) provides visibility into the IT and OT environments because attackers are looking to use IT environments as gateways into OT environments. Some companies may already have a network operations center monitoring the OT environment, but a combined SOC lets operators see all operations as they move through the network.
- **Design and Operate with Resiliency in Mind:**
  Resiliency and security can no longer be an afterthought. As new critical infrastructure systems are built and installed, legacy networks will be retired and taken offline. It is very important for next-generation systems to be built with resiliency and security in mind. The design and ongoing operation of the system must take into consideration what security threats will become commonplace in the months and years ahead.
- **Partner with Experts:** Be sure to partner with experts with vast knowledge of ICS threats. The public and private sector need to work together closely to protect this industry. Partner with a security company that can stay ahead of new threats and help operators address issues in real time.
- **Test, Test, Test:** It is critical that regular testing be a focal point in this sector. Tabletop exercises that enable a red and blue team to role play different catastrophic scenarios and the real time response to those scenarios is critical when having to have to deal with a threat in real time. Never underestimate the value of tabletop exercises in shoring up weakened defenses and helping executives understand the importance of security.

More can be done to reduce the ransomware risks during the holiday season and weekends, including:

- **Practicing good security hygiene** like implementing a security awareness program for employees, assuring operating systems and other software are regularly updated and patched, and deploying the best-in-class security solutions on the network.

- **Assuring key players can be reached at any time of day** as critical response actions can be delayed during weekend/holiday periods. It may be the case that the right people are not getting their emails due to system issues from the attack, or are not answering their phones because there is no set expectation, they need to monitor communications in case of an event. Having clear on-call duty assignments for off-hours security incidents is crucial here.

- **Conducting periodic table-top exercises and drills** and including those beyond the security team like Legal, Human Resources, IT Support and all the way up to the Executive Suite is also key to running a smooth incident response.

- **Ensuring clear isolation practices are in place** to stop any further ingress on the network or spreading of the ransomware to other devices. Teams should be proficient at things like disconnecting a host, locking down a compromised account, and blocking a malicious domain, etc. Testing these procedures with scheduled or unscheduled drills at least every quarter is recommended to make sure all personnel and procedures work as expected.

- **Evaluating Managed Security Services Provider (MSSP) options** if your organization has staffing or expertise shortage issues and establish pre-agreed response procedures with them so they can take immediate action following an agreed upon plan.

- **Evaluating lock-down of critical accounts for the weekend/holiday** when possible. The usual path attackers take in propagating ransomware across a network is to escalate privileges to the admin domain-level and then deploy the ransomware. Those highest privilege accounts in many cases are rarely required to be in use during the weekend or holiday breaks. Teams should create highly secured, emergency-only accounts in the active directory that are only used when other operational accounts are temporarily disabled as a precaution or inaccessible during a ransomware attack.

- **Deploying EDR on all endpoints.** The quickest remedy to the ransomware scourge for public and private sector businesses is deploying EDR on endpoints according to Gartner's Peter Firstbrook. Yet Firstbrook says that only 40 percent of endpoints have EDR.

- **Backing up all data and regularly testing those backups.** Maintain the backups of important files and regularly verify that the backups can be restored. Keep the backup files offline in case you are hit with a ransomware attack and the threat actors attempt to delete accessible backups.
- **Refraining from downloading pirated software/paid software offered for "free."** Remember – when a paid product is offered for free – you are the actual product
- **Not downloading software from dubious sources**

- **Not opening email attachments from unknown / unexpected sender**

For Help Evaluating Ransomware Risks, Contact:

CYBEREASON INCIDENT RESPONSE

Web: https://www.cybereason.com/services/incident-response
Phone: 855-695-8200

CISA

Email: central@cisa.gov
Phone: (888) 282-0870
Web: https://us-cert.cisa.gov

FBI

Email: CyWatch@fbi.gov
Phone: (855) 292-3937
Web: https://www.ic3.gov/