TIR-20241126 - Cyber Threats Don’t Take Holidays Off – Best Practices and an Aspire Case Study

11/26/2024

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

Table of Contents

Executive Summary **3**
Aspire Technology Partners Mitigates Thanksgiving Ransomware Attack **4**
Other Attacks **5**
Why Threats Increase During the Holiday Season **6**
Conclusion **7**
Aspire's Recommendations **8**
Aspire Protects **9**
MITRE Map **10**
Supporting Documentation **10**
Appendix II: Disclaimer **11**

Executive Summary

With the holidays right around the corner, it's important for businesses and organizations to stay mindful of the fact that cybercriminals see this jovial time as an opportunity for malicious acts. The hustle and bustle of the season—filled with celebrations, family gatherings, and spreading joy—can often lead to a lapse in keeping cybersecurity measures tight and vigilant.

Ransomware, malware, and phishing attacks tend to spike during the holiday season, putting sensitive data at risk. This rise in activity isn't just because more business happens online during this time. It's the result of more complex systems, stretched resources, and exploitable vulnerabilities all joining forces.

Let's explore how Aspire Technology Partners mitigated a ransomware attack during last year's Thanksgiving weekend and why it's important for your organization to prioritize strong cybersecurity best practices during the holiday season.

TIR Snapshot

- Aspire Technology Partners has had its share of thwarting attacks during the holiday season. We understand that the season is a time when most organizations face reduced staff and heightened cyber risks.
    - This fact became a reality when a customer was targeted by a sophisticated ransomware attack in 2023.
- During Thanksgiving 2023, attackers exploited a customer's vulnerable Cisco ASA VPN before slipping into the network unnoticed through the AnyConnect VPN client.
- Using a compromised domain admin account, they moved laterally across the environment, targeting critical systems.
- Aspire's Security Operations Center immediately sprang into action, collaborating with the customer's internal IT team and the Surefire Incident Response (IR) team.
- Aspire's investigation pinpointed the VPN exploitation as the root cause and identified the attackers' lateral movements through internal IP ranges.
- Aspire's team worked to assess the scope of the breach, identifying compromised accounts and affected servers like *Fileserv1 and Fileserv2*.
- To limit further damage, Aspire recommended and oversaw several containment measures such as shutting down the VPN and resetting accounts.
- Aspire's team worked closely with the customer and the Surefire IR team, maintaining transparency and sharing insights throughout the investigation.
- Aspire's vigilant monitoring and rapid response disrupted the attackers' attempts to extort a ransom from the customer.
- This incident is a testament to the importance of having a trusted cybersecurity partner like Aspire Technology Partners.
- By being proactive, businesses can minimize the risk of falling victim to costly cyberattacks during this busy time of year.

Aspire Technology Partners Mitigates Thanksgiving Ransomware Attack

Aspire Technology Partners has had its share of thwarting attacks during the holiday season. We understand that the season is a time when most organizations face reduced staff and heightened cyber risks. For one of Aspire's customers, this fact became a reality when they were targeted by a sophisticated ransomware attack. But thanks to the vigilance and expertise of Aspire's Security Operations Center (SOC), a potential catastrophe was contained and mitigated.

The Threat Unfolds

During Thanksgiving 2023, attackers exploited a vulnerable Cisco ASA VPN before slipping into the network unnoticed through the AnyConnect VPN client. Using a compromised domain admin account, they moved laterally across the environment, targeting critical systems.

On November 25th, suspicious activity involving a domain controller signaled that something was very wrong, prompting the customer to ask Aspire's SOC team for help. Despite the reduced staffing (typical of the holiday season), Aspire's SOC team immediately sprang into action, collaborating with the customer's internal IT team and the Surefire Incident Response (IR) team.

Rapid Response and Containment

The first step was to confirm the attackers' entry point and timeline. Aspire's investigation pinpointed the VPN exploitation as the root cause and identified the attackers' lateral movements through internal IP ranges. Aspire's team worked to assess the scope of the breach, identifying compromised accounts and affected servers like *Fileserv1* and *Fileserv2*.
To limit further damage, Aspire recommended and oversaw several containment measures:

- **Shutting Down the VPN** - By November 27th, Aspire ensured the vulnerable VPN was disabled, successfully cutting off the attackers' primary access.
- **Account Resets** - All admin accounts, including the compromised *account*, were reset, and a company-wide password reset process was initiated.
- **Server Rebuilds** - High-priority servers were restored from backups to minimize operational downtime.

Expert Coordination and Visibility

Aspire's team worked closely with the customer and the Surefire IR team, maintaining transparency and sharing insights throughout the investigation. Key findings, forensic data, and meeting notes were securely stored by Aspire, providing the customer with full visibility into the process.

By December 8th, Aspire and Surefire concluded their forensic investigation, confirming no new alerts tied to the incident. Aspire's vigilant monitoring and rapid response disrupted the attackers' attempts to extort a ransom from the customer.

Beyond Recovery - A Path to Resilience

Aspire's commitment to their customer didn't stop at containment. Recognizing the need for long-term resilience, Aspire guided the customer through remediation steps:

- **Strengthening Endpoint Security** - Aspire identified gaps in Carbon Black deployment and ensured isolated systems were either secured or disconnected.
- **Enhancing Network Design** - Aspire provided recommendations to upgrade devices and infrastructure, including implementing multi-factor authentication (MFA) to harden access controls.
- **Strategic Planning** - Aspire supported the customer in developing a robust remediation strategy, from system upgrades to ongoing password resets across all user, service, and vendor accounts.

A Trusted Partner During a Critical Time

This incident highlighted why having a trusted cybersecurity partner like Aspire Technology Partners is so important. Even during the holidays, when resources were stretched thin, Aspire showed dedication and expertise, keeping the customer protected from further harm.

Aspire's quick actions didn't just stop the attack—they helped the customer come out of it stronger, with a more secure infrastructure ready to handle future threats. When cyberattacks hit during vulnerable times, Aspire proves time and again that they're **always ready**.

Other Attacks

Major businesses like Kaseya, JBS, Colonial Pipeline, and FedEx have all suffered significant cyberattacks timed around holidays or major events. Take a look at some of the most infamous holiday and major event cyber attacks.

Christmas (2017)

Retailers faced heightened risk during the holiday shopping season, as demonstrated by the 2017 NotPetya attack. Although it targeted Ukraine, NotPetya disrupted global supply chains, impacting companies like FedEx and Maersk. FedEx relied on manual processes to continue operations, while Maersk's shipping systems were paralyzed. Retailers and shipping companies

struggled to recover during the critical Christmas season, with total losses surpassing $10 billion.

Fourth of July (2021)

Over the Fourth of July weekend of 2021, Kaseya, an IT management software company, fell victim to one of the largest ransomware attacks in history. The REvil ransomware gang exploited zero-day vulnerabilities in Kaseya's VSA product, impacting 1,000 businesses across 17 countries. REvil deployed ransomware to connected endpoints and initially demanded $70 million for a universal decryptor. The timing was deliberate, with researchers noting that REvil waited for the holiday weekend to maximize disruption.

Memorial Day Weekend (2021)

On Memorial Day weekend in 2021, JBS, a major U.S.-based food processing company, was also attacked by REvil. The ransomware infected servers in North America and Australia, forcing JBS to halt operations temporarily. Despite leveraging backups to restore systems, JBS paid an $11 million ransom to prevent further disruption. The attack highlighted the financial risks of ransomware and the potential for repeat targeting.

Presidential Election (2024)

During the 2024 U.S. Presidential Election, the Federal Bureau of Investigation (FBI) and the U.S Department of Human Services (DHS) issued warnings about various fraud schemes and cyberattacks targeting election-related systems and services. It was anticipated that financially motivated cybercriminals were a greater risk than state-sponsored threat actors from nations like Russia, China, or Iran.

The threat actors used tactics such as ransomware and DDoS (Distributed Denial of Service) attacks to disrupt election operations. These threat actors engaged in a range of schemes, from offering false promises of high returns on investments in fake campaign funds to sending fraudulent voter registration alerts to their targets. While there were discussions about Iran launching cyberattacks on the presidential campaigns of President Donald Trump and then Vice President Kamala Harris, no significant incidents occurred during their campaigns.

Why Threats Increase During the Holiday Season

There are several reasons why threats increase during the holidays and major events like Thanksgiving or The Presidential Election. Here are the most common reasons:

- **Increased Online Shopping** - With more people shopping online, especially during the holidays, there's a higher volume of transactions, making organizations more vulnerable to phishing attacks as cybercriminals target these transactions for potential financial gain.

- **Attractive Holiday Deals** - Retailers often offer significant discounts, and inflation-weary consumers are more likely to fall for offers that seem too good to be true. This creates an opportunity for scammers to impersonate legitimate businesses and trick shoppers, resulting in revenue loss and reputational damage for the affected companies.

- **Volume of Holiday Communications** - During the holiday season, organizations send out a large number of emails, including promotions, order confirmations, and donation requests. This influx of messages provides scammers with the perfect environment to launch phishing attacks that can easily go unnoticed.

- **Reduced Staffing and Cybersecurity Coverage** - As more employees take time off, fewer individuals are available to monitor and respond to potential cyber threats. This leaves remaining staff more vulnerable to phishing scams, especially when security teams may be operating with limited resources during the holiday season.

- **People are Distracted** – Threat actors often exploit major events—like the Super Bowl, Grammy Awards, or natural disasters—when they know people are distracted. These moments of heightened excitement or crisis provide an opportunity for attackers to time their operations strategically, knowing that individuals and organizations may be less vigilant and less focused on security.

Conclusion

The holiday season brings a unique set of challenges for organizations, with the increase in online activity, tempting promotional discounts, and staff taking time off creating the perfect environment for cybercriminals to strike.

As consumers and businesses are bombarded with shopping deals, emails, and other communications, it's easier for phishing scams and other attacks to slip through the cracks. To stay ahead of these threats, organizations need to reinforce their cybersecurity efforts, keep employees informed about potential risks, and maintain vigilance, even when resources are stretched thin. By being proactive, businesses can minimize the risk of falling victim to costly cyberattacks during this busy time of year.

How is your organization preparing to defend against cyber threats this holiday season?

Aspire's Recommendations

Both the FBI and CISA have issued guidelines on how cyber security best practices can help organizations mitigate the risks, particularly ransomware and phishing attacks. Several of the recommendations from the FBI and CISA apply to how Aspire Technology Partners responded to the security threat involving their customer during 2023's Thanksgiving weekend. Here are some ways those best practices align with Aspire's actions during that time:

- **Ransomware Threat Monitoring** - Aspire's proactive approach to monitoring the situation with their customer, including working with Surefire IR Teams, reflects the CISA and the FBI's recommendation to continuously monitor for ransomware threats during high-risk times, such as holidays and weekends. By staying involved throughout the entire investigation, Aspire helped the customer mitigate potential damages.

- **On-call IT Security Staff** - Aspire's ongoing involvement in the incident, with meetings and updates spanning from 11/26 to 12/8, demonstrates the importance of having dedicated IT security personnel on standby during critical times. Having experts available during a security incident ensures timely action and reduces the risk of escalation.

- **Backup and Recovery Procedures** – Aspire recommended that the customer utilize their backup procedures. As a result, the customer worked on remediation efforts—including identifying systems without Carbon Black and strengthening their backup and recovery process. This aligns with the CISA recommendation to maintain offline, encrypted backups and regularly test them.

- **Phishing Awareness** - Aspire emphasized the importance of user training and phishing exercises to their customer. Remember, phishing is often the initial vector for ransomware. The recommendation to raise awareness about phishing attacks is a key part of the broader cybersecurity measures Aspire supports for its clients.

- **Incident Response Plan** - Aspire's methodical and organized response, including the documentation of investigation notes, emails, and action steps, mirrors the CISA recommendation to maintain a cyber incident response plan. Aspire helped the targeted customer develop and implement procedures to respond to and contain the threat.

- **Multi-Factor Authentication (MFA) and Network Security** - As part of the ongoing remediation efforts, the customer immediately started working on the implementation of MFA and network upgrades. This recommendation is an integral part of reducing the risk of successful attacks and improving overall network security, which aligns with Aspire's advisory role in improving security practices.

By following these best practices, you can better protect your systems, data, and networks against cyber threats. For CISA and the FBI's complete list of recommendations, please see their advisory.

Aspire Protects

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

MITRE Map

Aspire Technology Partners Case Study MITRE Map

Initial Access	T1190 – Exploit Public Facing Application T1078 – Valid Accounts
Persistence	T1133 – External Remote Services T1562.001 – Disable or Modify Tools
Credential Access	T1110 – Brute Force T1528 – Steal Application Access Token

Supporting Documentation

JOINT CYBERSECURITY ADVISORY

How to Protect Against Cybersecurity Threats This Holiday Season

Why Scammers Love the Holidays, and How to Stop Holiday Phishing Risks

What are the main cyber risks and threats this festive season? | TSC

Ransomware Awareness for Holidays and Weekends | CISA

The 3 Most Prevalent Cyber Threats of the Holidays

Why There Are More Cyber Attacks During Holidays? | RiskXchange

Inside Intelligence Center: Financially Motivated Chinese Threat Actor SilkSpecter Targeting Black Friday Shoppers

Don't Forget About Cybersecurity With Increased Telecommuting And The Holiday Season - Security - Technology - United States

Holiday Cybersecurity Tips | NCDIT

Holiday, Weekend Ransomware Attacks Continue to Hit Companies Hard

Here's why cybercrime spikes during times of global crisis | World Economic Forum

Holiday Cyber Attacks: Tips & Trends | ThreatLabz
This Holiday Season, Don’t Forget to Prepare Your Organization for Cyber-Threats - Infosecurity Magazine

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.