

**Cyber Attack White Paper**

*This white paper is being written as an overview of a cyber attack that occurred in November 2021. It is meant to provide details of the attack, how we responded and overcame the attack, general observations and lessons learned through the attack, and some corrective actions that we are planning to further strengthen our cyber security moving forward. There is a lot of talk about cyber security but not as much granular detail – so I am looking to share nuggets that I wish I had known prior. I hope that it is informative and useful. – Brett M. Mears, President*

**General Information**

Threat actors (or malicious actors) are people or groups that take part in actions that intend to cause harm in the cyber realm. They often operate in countries that endorse, or overlook, the criminal activities, such as Russia, Iran, and North Korea. We learned through the Federal Bureau of Investigation (lead federal agency for investigating cyber attacks and intrusions) that cyber attacks are occurring in the US at the rate of one every eight seconds. The threat actors target sensitive industries like hospitals during COVID peak demand, energy industry during winter demand, or supply chain during demand challenges to increase the likelihood of extorting money from businesses. At a recent IWLA (International Warehouse & Logistics Association) conference in Q4 2021, my informal polling tallied approximately one in five warehouse 3PLs as having been attacked by ransomware in the past two years. In our case they used malware (malicious software) to infiltrate our computer network to access data, encrypt data, and deny the use of our network.

**Attack Overview**

From our best deduction we believe the attack started with a spoofed email where the threat actor (TA) sent a company employee an email that appeared to be from an actual customer. Although in review there were some suspicious aspects to the email, our employee accessed the link within the email even though the email gateway did strip out the “bad” hyperlink (employee cut and pasted the URL to their web browser). This link downloaded malware to the employee’s local computer that then propagated using cached credentials. Despite having the latest builds of Trend Antivirus (AV) and Endpoint Detection and Response (EDR), which successfully identified the malware, the TA was able to bypass (beat) the AV and EDR.

On November 1, 2021 the TA used a Cobalt Strike tool in conjunction with RClone to access our network. This initial access was not detected. Two days later on November 3, 2021 they deployed their ransomware in the early morning. When the team arrived in the morning, they could not access the network due to the Denial of Service DNS attack. Within minutes the ransomware attack was realized and we activated our incident response plan, took our network offline, and began an investigation. In our case the perpetrator was Conti, a Russian ransomware gang.

**Initial Response & Recovery**

We immediately filed a claim with our insurer, HDI Specialty Insurance, who assigned a team of external cybersecurity professionals experienced in handling these types of incidents. A privacy attorney, McDonald Hopkins PLC, was assigned and they brought in Tetra Defense, a computer forensics firm, on our behalf to thoroughly investigate the nature and scope of this incident and the security environment. Tetra oversaw deployment of Sentinel One, an industry-leading endpoint detection and response tool, throughout Palmer’s environment to collect evidence and to ensure the security of systems as they were purposefully brought back online. Sentinel One is monitored continuously 24/7.

As forensics IT worked to better understand the attack and protect us moving forward, Palmer IT began recovery efforts immediately:

* Connections with external partners were shut down (Zethcon, Azure, etc.)
* A temporary replacement server was obtained to ensure a clean environment.
* Impacted critical application systems were restored using backups from October 2021, prior to the date of incident and any observed indicators of compromise.
* A new domain with completely new user accounts was deployed, restored, and rebuilt. Systems were re-added to the new domain. New user accounts now use complex username, higher complexity password, and no associations.
* Non-critical servers and workstations were replaced or rebuilt from factory defaults; applications were reinstalled and, when necessary, user and application data was migrated back to these systems from backups.
* VPN and External access were limited to IP address ranges owned by Palmer, and approved vendors.
* All MS Office 365 applications were elevated to E5 Multi-factor Authentication
* Added mail security protocols with all inbound email forwarded to Trend Micro Security Server before entry into Palmer Logistics’ MS Office 365 platform.
* All endpoints from Palmer networks were replaced with new endpoints.
* Disks replaced, or partitions removed, and re-imaged with the latest Windows 10 Pro, all patches applied.
* No legacy accounts, associations, or references to the previously compromised environment.
* Phone system server (Voice over Internet Protocol) was completely rebuilt and redeployed.

Palmer systems went down completely the morning of Wednesday, November 3rd. We immediately launched our Business Continuity Plan and started recovery. Remote hosted systems were able to be brought back first. Some (Zethcon Synapse) could be accessed immediately via VPN outside the company network. Others (NAV, Great Plains) came back mid-way through the following week. The locally hosted applications took longer, and most were back online by the end of the next week, November 12. Concurrently IT was collecting all hardware to either replace or rebuild, install required applications, and initialize for secure user access. That process was augmented with contractor labor but still took approximately a week to fully complete. By Monday, November 22, Palmer was restored to normal operating capacity; for 2.5 weeks we were significantly impacted in our ability to operate. During recovery we continued to receive all inbound shipments normally (although some customer reduced or diverted inbounds). We shipped emergency orders, or non-impacted customer system (not on our network) shipments daily. As a company (considering inbound & outbound activities) we operated approximately as follows:

November 3 – 8: 63% operational

November 9-11: 68% operational

November 12-16: 74% operational

November 17-21: 79% operational

November 22 and after: 100% operational

Fortunately, we were able to catch up with entering documented inbounds and most customer backlogged orders prior to the end of November by extending hours and working on the remaining weekend.

**Lessons Learned**

* Ransomware – in some cases you are prevented by law from even paying the TA (under US Dept of Treasury’s Office of Foreign Assets Control).
* Paying the TA is no guarantee that the situation will be resolved (quickly). TA’s usually provide the decryption key that will take time and will likely damage your data during decryption.
* You shouldn’t have your cybersecurity insurance policy on your network drive as the TA will then know how much you are covered for and they will likely put the ransom just slight under your coverage limit.
* “Defense in Depth” (personnel, procedural, technical and physical security) is critical to ensure adequate layers of protection when one security layer fails (in our case personnel training).
* Almost 1 in 2 companies hit with ransomware actually pay the ransom. The ransom is negotiable.
* You should commission an outside firm to do an IT Security Risk Assessment periodically.
* Given pandemic and supply chain challenges, it is wise to have excess/contingency hardware, as recovery time to get back on line after a cyber attack will be exacerbated by lead time issues on equipment.
* Communication to customers was complicated with both email and VoIP phone system knocked out due to cyberattack.
* Cloud or remote hosted applications were able to recover much faster than older local networks.
* We needed to better leverage our applications (One Drive, Teams, Sharepoint) to reduce reliance on local servers.

**Next Steps**

* Hire IT consultant to conduct an external Security Risk Assessment (SRA)
* Review, update, and expand Business Continuity Plan for Cyber Attack incorporating lessons learned.
* Assess cyber security training program and make improvements to better educate and prepare employees for the risk of cyber attacks.
* Establish monthly training and phishing exercise program for all employees.
* Implement a proxy server for web access.