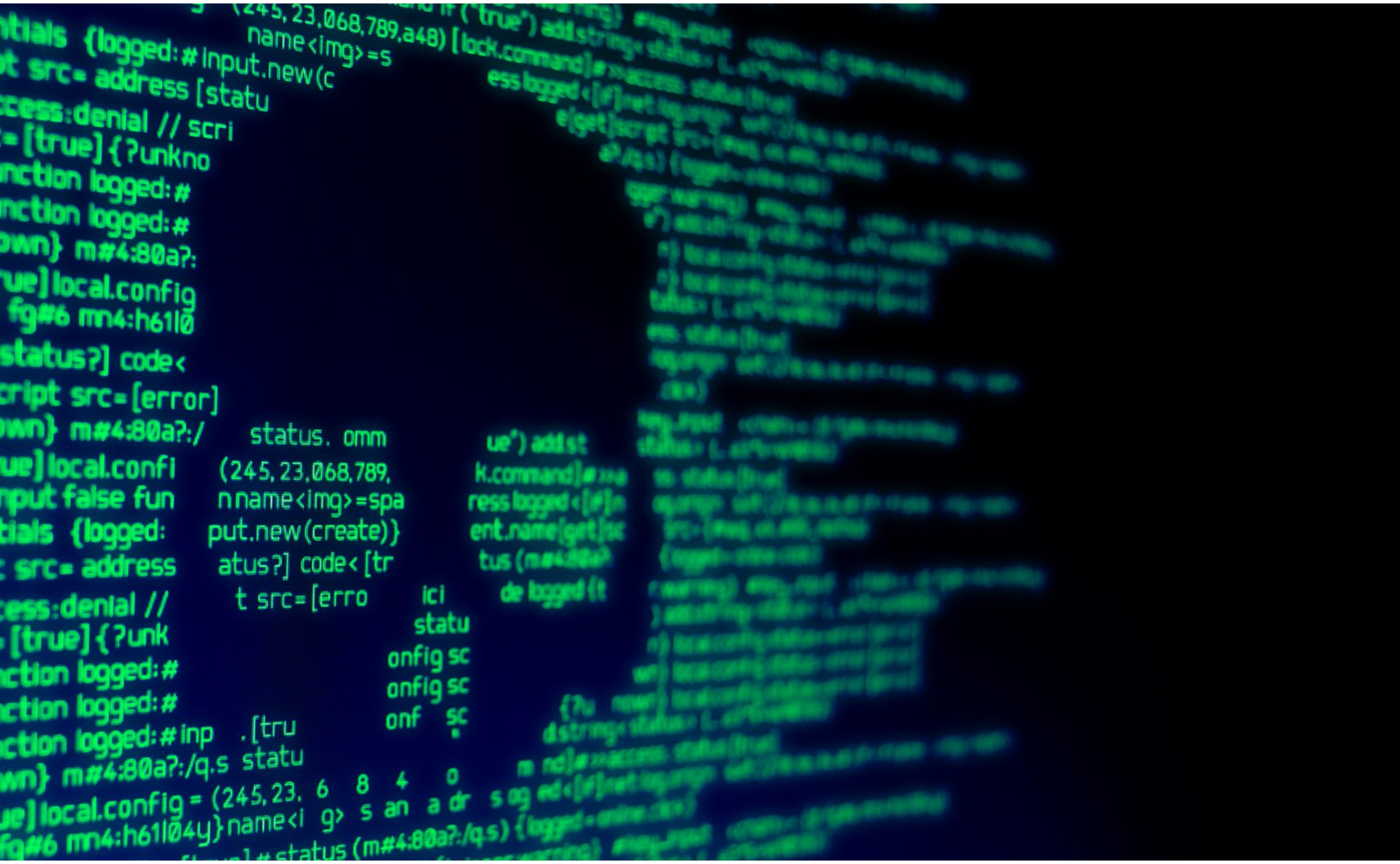

Case Study: Tevora Ransomware Incident Response

As the frequency and sophistication of ransomware incidents continue to escalate, it's more important than ever to identify partners that can help fortify your defenses against these insidious attacks and minimize financial and operational impacts when they occur.

This case study describes how Tevora helped an industry-leading sports apparel company to quickly diagnose a significant ransomware attack, remediate damages, restore systems to normal operation, and shore up defenses against future attacks.

To protect our client's confidentiality, we'll refer to them by the fictitious name of Sports Apparel International (SAI).

Dead in the Water

In late 2019, SAI began experiencing significant problems on multiple systems across their global network. Their in-house security team determined that a large-scale malware incident had occurred and that virtually all machines in their network—including 32 domain controllers—were infected with the Ryuk ransomware.

Ryuk and other similar ransomware variants encrypt the hard disk of infected systems, rendering them inoperable. Once the systems are infected, the malicious software is difficult to stop because it launches multiple instances of the encryption process, which in turn allocates all memory and CPU, preventing users or administrators from stopping the attack.

The incident left SAI's retail and manufacturing systems dead in the water, completely hobbling their ability to sell and manufacture products.

A Call for Help

Realizing their situation was dire, SAI called Tevora for help. We immediately deployed our incident response team to begin diagnosing the ransomware and identifying ways to get SAI back up and running as quickly as possible.

Analysis

Tevora partnered with the SAI security team to perform the following initial analysis activities:

- Captured disk images of key domain controllers.
- Analyzed malware to determine its capabilities and how the infection spread.
- Identified Indicators of Compromise (IOC) —the digital footprints left behind by the attackers.
- Provided IOCs to Trend Micro—SAI's endpoint protection partner—so they could immediately be added to blacklist systems to defend against future attacks using the same malware.

Malware Designed to Avoid Detection

The initial analysis indicated the Ryuk ransomware was distributed out to the global network via three group policies that were set up at the root domain controllers. The attackers obtained credentials for an Australian admin user id with elevated privileges and leveraged them at the root domain level to put the three group policies in place. These policies placed "net.exe" and variants of "1.exe"—renamed using randomly-generated names—on targeted systems, then set up scheduled tasks that would run repeatedly on the endpoints. The randomly-generated names enabled the malicious .exe files to avoid detection by SAI's blacklisting anti-virus applications.

IOCs Developed to Guard Against Future Attacks

While the malicious .exe files had different names on each infected system, they had consistent IOCs, including use of the same SHA-256 hash value. Using these IOCs, in combination with other unique properties of the malware, Trend Micro was able to develop a signature and deploy it on SAI's blacklisting anti-virus applications to protect existing and newly-installed systems against similar future ransomware attacks.

Sophisticated, Customized Malware

Tevora determined that the malware was able to gather information about the SAI systems environment and write it to a database file. We also identified parts of the malicious software that were hardcoded with specific SAI resource names, including valid host and domain controller names. This suggests that the attackers had access to the SAI environment for at least a day or two before the attack, and were able to use this time to gather information and use it to develop customized ransomware targeted at the SAI environment.

Multi-Million Dollar Ransom Payment Demanded

The malware files on infected systems contained instructions to contact the attackers at a provided email address to get details on the ransom payment required to decrypt SAI's disks. SAI engaged Flashpoint—a firm with considerable experience negotiating with ransomware threat groups—to interact with the attackers.

Before contacting the attackers, Flashpoint reviewed Tevora's malware analysis and IOCs and concluded that the ransomware was associated with a credible threat group with a reputation for honoring their commitment to decrypt systems after receiving the demanded ransom payment. Next, they reached out to the attackers via email, and subsequently via a chat connection, and learned that a multi-million-dollar Bitcoin ransom payment would be required to unlock SAI's systems.

After learning of the large ransom amount demanded, SAI's management asked Tevora and their other technology partners to determine if there was a way to restore their systems to normal operations without paying the ransom, and if so, how much it would cost.

```
;j<8;j++){
ece = $('piece_'+i+'_'+j);
or=='black' && piece &&
 Draggable('piece_'+i+'
 (color=='white' && piec
 Draggable('piece_'+i+
 es.add('square_'+i+'
 t: 'piece',
 ass: 'active',
 · function(piece,
```

A Plan to Build a Parallel Network

Working in collaboration with SAI and its partners, Tevora quickly developed a plan for rebuilding SAI's global network of retail and manufacturing systems on a parallel set of malware-free systems.

The first phase of the plan would involve rebuilding SAI systems on new, clean servers. SAI Blacklisting applications would be updated with the newly-developed ransomware IOCs to guard against re-infection. Each new server would be closely monitored for re-infection for 48 hours before greenlighting it for production operation.

In a second phase, infected machines would be wiped clean, reinstalled, then brought online after the 48-hour monitoring period. Systems would be brought back online on a region-by-region basis, with careful monitoring before expanding from one region to the next.

Return to Normal Operations

After weighing the pros and cons, SAI management elected to go with the parallel network plan and not pay the ransom. This set in motion an intense, collaborative effort between SAI, Tevora, and SAI's other technology partners to implement the parallel network.

Using a follow-the-sun approach, with daily global team checkpoints, the team was able to restore SAI's retail systems to normal operation, free of malware, within one week of the attack. Manufacturing operations were back online within two weeks of the attack.

Financial Impacts

SAI was extremely pleased to not have to make the ransom payment—and to avoid the risk that their systems would not be successfully decrypted after the payment was made. However, they still incurred significant costs, including:

- Lost revenue due to retail systems being offline for one week, and manufacturing for two weeks.
- Costs to engage Tevora's incident response team, Flashpoint, and other technology partners involved in diagnosing the ransomware and implementing the parallel network plan.
- Legal costs to ensure compliance with data privacy laws during implementation of parallel network, including compliance with European GDPR laws.
- Costs to offset reputational damage associated with attack, including a communication campaign to assure customers that their data was safe and that systems would be back online soon. This also included costs for offering a 10% discount to incent customers to make purchases following the attack.

Recommendations

After SAI's systems were returned to normal operation, Tevora made a series of short-term and long-term recommendations for shoring up SAI's defenses against future cyberattacks.

Short-Term Recommendations

- Rotate passwords and any encryption keys.
- Terminate infected workstations and reimage them.
- Update all systems being put into production, and ensure they have the latest Microsoft Windows patching. This will help prevent attacks such as EternalBlue, which is used by Ryuk and other ransomware.
- Deploy endpoint protection (EP) such as next-gen anti-virus (NGAV) to all systems before being placed into production, and ensure EP has the latest signatures to help prevent future infections.
- Deploy endpoint detection and response (EDR) to help monitor recovery efforts. If any new infections occur, EDR can isolate the infected host so the team can take it down to reimage it.

> "…the team was able to restore SAI's retail systems to normal operation, free of malware, within one week of the attack. Manufacturing operations were back online within two weeks of the attack."

Long-Term Recommendations

- Conduct quarterly security awareness exercises for all staff. Exercises should include easy to hard detection levels for phishing emails.
- Enable multi-factor authentication throughout the organization, wherever possible, with an emphasis on email and web access to company resources.
- Perform an annual penetration test across the entire external network infrastructure to identify potential points of entry for attackers.
- Perform an annual penetration test across the entire internal network infrastructure.
- Run quarterly vulnerability scans against all external or internet-facing endpoints.
- Review firewall rules annually or after any significant network changes.
- Consolidate all logging and monitoring in a central location. Implement security event information monitoring with staff that has the skills and abilities to decipher security events and respond properly.
- Implement and regularly update a next-generation anti-virus solution with the ability to detect known signatures and bad behavior across the entire global environment on all instances.
- Implement system administrator jump boxes with multi-factor authentication enabled on them. These should only be used for domain admin and/or administrator purposes. This will significantly hinder an attacker's ability to escalate privileges within the environment.
- Implement a "Zero Trust" architecture in which every person or device accessing a company resource is verified, regardless of whether they are inside or outside of the company's network perimeter. This is a broad concept, which includes things such as:
    - Using multi-factor authentication to verify all users accessing company resources.
    - Establishing granular network segmentation and only allowing users that need access to perform their work to access a specific network segment.
    - Using the concept of "least privilege" to grant tiers of user access rights and privileges so that users are only granted the access rights and privileges needed for their job.

Let Tevora be Your Trusted Partner

Tevora's expert team of security specialists can partner with you to help build up your defenses against ransomware and other cyberattacks. This includes reviewing your environment for potential security weaknesses, implementing tools and techniques to protect your environment, and training your staff to be aware of emerging ransomware, phishing, spearphishing, and social engineering trends, so they are fully equipped to be the first line of defense against attack.

If you do suffer a ransomware or other type of cyberattack, Tevora's experienced incident response team can jump in at a moment's notice to help you get back up and running quickly, while minimizing financial, operational, and reputational damage.

If you'd like to learn more about how Tevora can be your trusted security partner, just give us a call at **(833) 292-1609** or email us at **sales@tevora.com**.