TEVORA™

Case Study

# Cracking the Code:

## Tevora Helps Building Materials Manufacturer Respond to Sophisticated Fake Browser Update Ransomware Attack

**Option 2-Disguised Browser Update:**

**Tevora Responds Against Advanced Ransomware Attack**

As many organizations have learned to defend against common ransomware attacks successfully, cybercriminals are shifting tactics to use increasingly sophisticated ransomware techniques. Identifying partners that can help strengthen your defenses against and respond to emerging ransomware threats is more critical than ever.

This case study describes how Tevora helped an industry-leading building materials manufacturer to quickly diagnose and remediate a sophisticated ransomware attack that gained access to their systems via a seemingly innocuous fake browser update prompt.

To protect our client's confidentiality, we'll refer to them as Building Materials International (BMI).

## Attack Originates at Watering Hole

The attack originated when one of BMI's satellite office employees visited a WordPress event website to research potential venues for their upcoming holiday party. Unfortunately for BMI, the site had been compromised and turned into a watering hole, waiting for unsuspecting users to visit.

SocGholish javascript malware had been installed on the compromised site. This malware looked for users who left their browser open for an extended period after visiting the site. When the malware detected such a victim, it was designed to switch the whole page to a fake Google Chrome browser update prompt. When a victim clicked on the apparent browser update, the malware was programmed to download a sophisticated ransomware payload to the victim's system.

## A Fateful Click on a Seemingly Legit Browser Update

The BMI employee visited the compromised WordPress site during working hours, then left their browser open for the rest of the day and did not close it when they went home for the evening. That night, after observing an extended period of inactivity on the employee's open browser, the watering hole malware installed malicious software that prompted the employee to perform a browser update.

The following morning, when the employee came to work, they noticed the seemingly legit prompt to update their browser and clicked on it. This triggered the javascript malware to install ransomware on the employee's workstation, which encrypted their hard disk, locking them out completely. The malware displayed a message demanding payment of $750,000 to restore the encrypted data, not disclose stolen data, and not launch a denial of service (DoS) attack against BMI. The message also provided instructions for payment in Bitcoin.


## BMI Calls for Help

BMI's Microsoft Defender antivirus software detected the encryption and malware and alerted their security staff. After an initial diagnosis effort, the BMI security team was unable to determine if the malware had spread to other parts of their environment or how the BMI employee's workstation had become infected.

BMI's security team realized they needed enhanced expertise and called Tevora for help.

## Tevora Responds

BMI called Tevora's 24-7 hotline, and within minutes, our security and malware experts began working with BMI's security team.

## Rapid Diagnosis

Tevora partnered with BMI security staff to rapidly gain a comprehensive understanding of the malware, its deployment, and any additional BMI systems that may have been impacted.

We first identified the malware on the BMI employee's workstation and removed it to prevent it from spreading to other parts of the BMI network.

Next, we reviewed logs of the BMI employee's activity, looking for recent visits to known malicious websites, but could not find any indication of such visits. However, could identify the attacker's IP addresses, which we could link to the watering hole event website. This solved the mystery of where the attack originated.

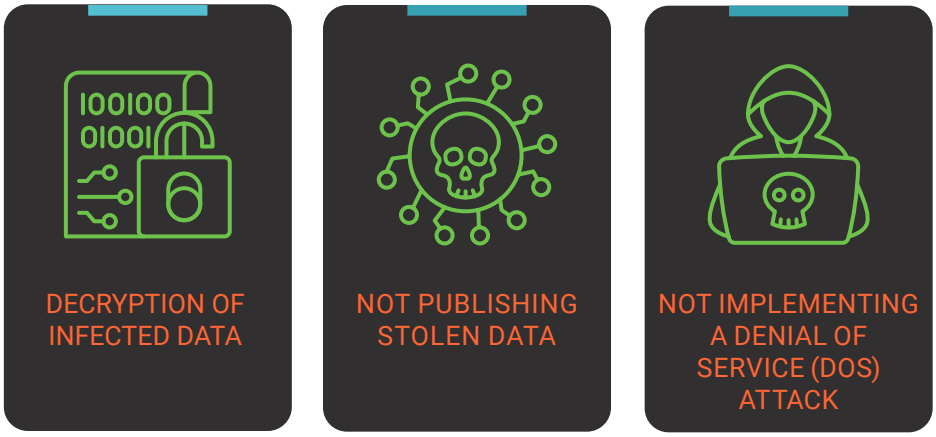
After analyzing the malware and manually reviewing all endpoints in BMI's environment, we determined that the malware did not appear to have been spread beyond the employee's workstation.

## Sophisticated Malware

We determined that it was sophisticated by reviewing the watering hole malware and the forensic footprints it left on BMI systems. Here are some of the key things we learned:

- The "Stage 1" SocGholish malware running on the watering hole site was designed to download a Remote Access Trojan (RAT) to the victim's system. The download RAT was Cobalt Strike, a paid penetration testing product that allows attackers to deploy an agent on the victim's machine. While Cobalt Strike can be used for legitimate penetration testing purposes, malicious actors can also use it, as in this incident.
- The SocGholish malware detected the victim's browser type (e.g., Edge, Chrome, Firefox) and default operating system language (e.g., English, Spanish, French) and used that information to display a realistic fake browser page to the victim.

- Cobalt Strike installed BlackCat ransomware on the BMI employee's workstation when the victim clicked on the fake browser prompt. This ransomware is sold and operated by ALPHV, a Russian-speaking cybercrime organization. The malware uses a triple extortion tactic, demanding a Bitcoin ransom payment for:




To Pay or Not to Pay? After confirming that the malware had been contained, we helped BMI management through the decision of whether to pay the ransom or not. Based on our input and guidance, BMI decided not to pay the ransom. In addition to a general sentiment of not wanting to reward the attacker's bad behavior, we felt that BMI's risk of adverse impacts was minimal because:

- They had a recent backup of the BMI employee's workstation data, which could be easily restored.
- The data on the employee's laptop was not particularly sensitive and, as such, would not present any significant risk to BMI if the attackers publicly disclosed it.
- They had recently taken steps to fortify their defenses against DoS attacks, including:

**Implementing traffic filtering and rate limiting to filter and block malicious traffic and limit the requests allowed from a single IP address.**

**Using Content Delivery Networks (CDNs) to distribute traffic across a network of servers to improve their ability to absorb and mitigate the impacts of DoS attacks.**

**Implementing load balancers to balance load across multiple servers evenly, reduces the risk that a single server would be overwhelmed during an attack.**

## Remediation

To guard against the possibility that some malware had gone undetected, we recommended that the BMI employee's workstation hard disk be wiped. While that process was happening, the employee was given a new workstation with data restored from a recent backup. The whole process took less than a day.

After being wiped, the employee's old workstation was reimaged and assigned to a new employee.

In an abundance of caution, we also worked with BMI to disconnect other workstations in the impacted satellite office and supply those users with new workstations. Their potentially-impacted workstations were wiped, reimaged, and reused for other purposes.

We also identified the IP addresses the remote attacker usedand partnered with BMI staff to use firewalls to block these addresses and associated URLs.

## Return to Normal Operations

After completing the remediation work, BMI returned to normal operations with minimal business impacts. With Tevora's help, this occurred within two days of the ransomware attack.

## No Indication of Further Malicious Actions by ALPV

As of the writing of this blog post, BMI has not experienced any follow-up attempts by ALPHV to disclose stolen data. This may be because ALPHV realized that any data stolen from the employee workstation was not sensitive and would not be worth using in an extortion attempt.

Similarly, there has been no indication of a DoS attack directed at BMI. This may be because ALPV determined that BMI's DoS defenses were sufficient to render a potential DoS attack ineffectual.

## Key Takeaways

In many ways, BMI dodged a bullet with this incident, thanks to their defensive actions before the attack and their decision to partner with Tevora to quickly diagnose and contain the attack. Had they not done these things, the attack would likelyhave resulted in significant and potentially catastrophic financial and operational impacts.

Key Achievements in BMI's Response In reviewing the incident, we believe there are many things BMI did well to prepare themselves for this type of ransomware attack and to respond effectively when the attack was detected, including:

- Use of Microsoft Defender on their endpoints. This provided an early warning of the malware and encryption activities on the BMI employee's workstation. It also enabled them to engage Tevora in time to help contain the malware in the employee's workstation, avoiding broader infection. It's also worth noting that they regularly applied Defender updates to ensure it was current and could detect emerging malware threats.
- Early realization that they needed more expertise than existed on their Security team and their decision engage Tevora immediately.
- Effective backup and restore tools and procedures enabled them to recover the data encrypted on the BMI employee's workstation.
- Proactively Implement traffic filtering, ratelimiting, CDNs, and load balancers to strengthen defenses against DoS attacks.

## Strengthening: Identifying Opportunities for Enhanced Fortification

We also identified opportunities to strengthen their defenses, outlined in our BMI management report at the end of our engagement. These included:

- Enhanced security awareness training for BMI staff, including an emphasis on the importance of closing browsers when not in use and education on detecting the latest fake browser update attack malware, including SocGholish, RogueRaticate/ FakeSG, ZPHP/SmartApeSG, and ClearFake.
- Incorporation of the open-source Emerging Threats Ruleset to help detect and protect against new and previously unknown malware, including fake browser update malware.

## Additional Resources

Below are additional resources that provide a deeper dive into topics covered in this case study:

- Krebs Fake Broswer Update Article
- Proofpoint Article on Fake Browser Updates
- Tevora Ransomware Preparedness Services
- Tevora Emergency Incident Management and Response

TEVORA™

## We Can Help

Tevora's team of experts can answer any questions about preparing for and responding to fake browser updates and other ransomware attacks. Reach out to our team at (833) 292-1609 or email us at sales@tevora.com.