Cobalt Strike infection

> In this case, we look at a hospital that very nearly fell victim to a ransomware attack called 'Cobalt Strike.'

The rise of ransomware in recent years has varying implications for businesses across industries. In this case, we look at a hospital that very nearly fell victim to a ransomware attack called 'Cobalt Strike.' Luckily, the hospital was insured by CFC and our cyber threat analysis team was one step ahead of the hackers, helping to prevent the attack before it happened.

Shared intelligence identifies a target

CFC works with a variety of third-party partners including law enforcement organizations, intelligence agencies and innovative private sector partners who share information and intelligence about cyber threats happening around the world.

In this case, a partner that monitors exposed command and control servers helped us identify that one of our insureds, a children's hospital in Texas, had a malicious piece of malware installed on their systems. They did this by sharing a list of compromised IP addresses, domains and hostnames which our cyber threat analysis team then compared against our own list of cyber insureds.

Once the hospital was identified, the team established that it had been tagged with the Cobalt Strike beacon.

Understanding Cobalt Strike

Cobalt Strike is a penetration testing toolkit created by ethical hackers but is now used by malicious actors due to its efficiency and ease of use. It allows the attacker to place an agent, called a beacon, on a target network. From there, Cobalt Strike enables an attacker to perform a number of exploitations and attacks. These include command execution, key logging, file transfer, privilege escalation, lateral movement, malware execution, and many others.

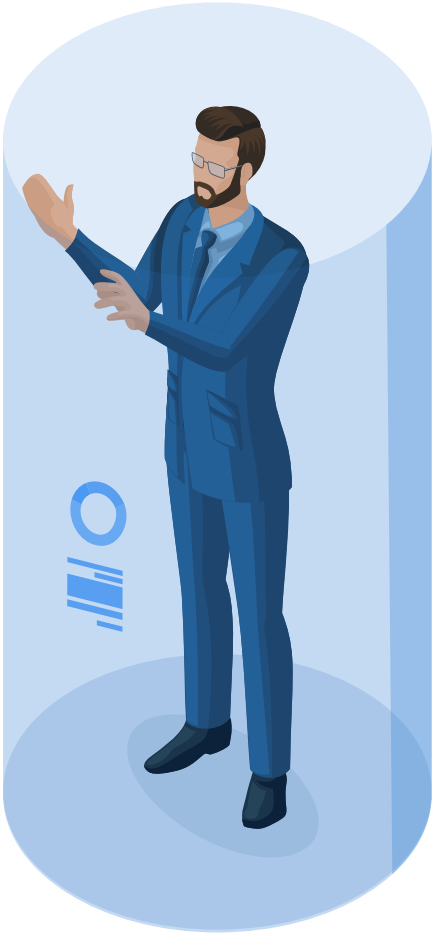
This type of attack usually ends in malicious malware shutting down systems, data exfiltration and extortion, resulting in significant business interruption. For a hospital, business interruption of this magnitude could cost lives, which makes them a likely target for higher than usual ransomware demands.

Remediating the threat

Using our incident response app, our cyber security team immediately notified the insured and our team was able to remove the foothold that the attacker had in the environment.

First, they entered the insured's environment and isolated the infected devices, limiting the attacker's ability to spread throughout the environment and cause more damage. They then deployed tools into the environment that hunted for known indicators of compromise and used the threat intelligence supplied by the cyber threat analysis team and our partners to thoroughly purge the system of the attackers, including removing any backdoors and other persistence methods.

Once the system was purged of the malicious actors, they worked with the insured to block other known command and control servers on their firewall and reduce the likelihood of future attacks.



Ransomware averted

Given what we know about the use of Cobalt Strike - and what our team observed on the victim's system - the attacker was likely attempting to exfiltrate data and execute a ransomware attack.

Healthcare institutions and hospitals like this insured carry a significant cyber exposure due to the severity of the impact that could occur if their systems are compromised. Ransomware attacks on hospitals of a similar profile usually incur a ransom demand of between £2 million - £8 million.*

*Based on calculation from CFC's ransomware calculator.