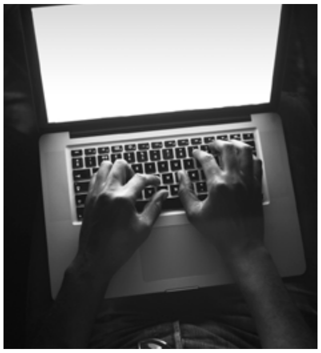
AVALON Cyber

# **Case Study:** Incident Response – Cybercriminal nearly gains access through third-party vendor application



Avalon Cyber was able to thoroughly examine the behaviors and identified that the attacker executed obfuscated code

## The Incident

Avalon Cyber received multiple Managed Detection & Response (MDR) alerts about potentially malicious system behavior occurring on several of our client's network and systems. The suspicious activity consisted of an application executing obfuscated code via PowerShell (a Microsoft tool that automates administration tasks)—one of the telltale signs of criminal activity.

## The Plan

To perform digital forensic incident response (DFIR) and threat hunting activities on systems for purposes of identifying unusual behaviors and determining legitimacy of activities identified within the client's network and systems.

## The Investigation

Avalon Cyber performed a thorough analysis of the process "kill chain" (the phases of a cyberattack) and determined that a remote system support utility, called Bomgar (an application IT administrators use to remotely manage and support computer systems), was initiating the identified suspicious behaviors.

While our client doesn't use Bomgar, they mentioned that one of their vendors uses the program to manage and maintain the systems running their customers' (including our client's) on-premise applications.

Through our DFIR analysis, Avalon Cyber was able to thoroughly examine the behaviors and identified that once the bad actor obtained access to the hosts via Bomgar, the attacker executed obfuscated (Base64) code via PowerShell. We were able to decode the script and identified that it was attempting to reach out to PasteBin (a website where text can be stored and shared) to retrieve weaponized code to carry out the remaining steps in the kill chain (exploitation, installation of malware, establishment of command and control, and objectives).

Avalon Cyber was able to block the malicious activity before serious damage could occur. However, not all systems had our sensors installed, thus, the attack was not identified by the other systems that only had traditional antivirus installed. Given this, we continued our investigation to determine the impact of the incident.

Using a sandbox (a technical term for a safe system to analyze application behavior), the Avalon Cyber team was able to identify that the weaponized code from PasteBin would have, indeed, established a command and control connection back to the adversary. Furthermore, attacker toolkits like PowerSploit would have been deployed to further exploit information from our client's systems and possibly move laterally within the client's network systems.

## The Result

Our team successfully foiled the attempted cyberattack, which ultimately could have led to loss of our client's protected information, database manipulation, ransomware installation, and other nefarious actions.

AVALON Cyber

## QUESTIONS?

For more information on Incident Response or any of our services, please contact:

**Ian Gattie**
Director of Marketing
716.995.7777
ian.gattie@teamavalon.com