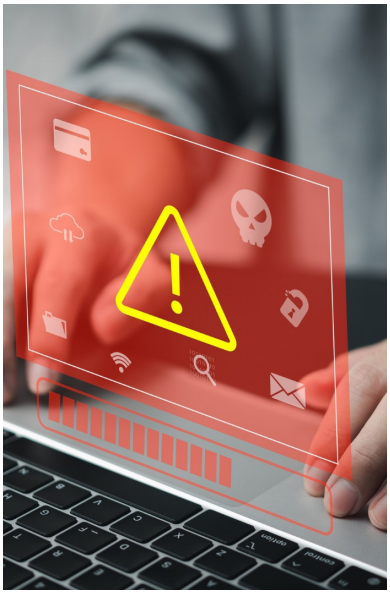
Case Study: Incident Response



Avalon's managed detection and response (MDR) platform detected a series of alerts indicating potentially malicious behavior across multiple systems within a client's network. The activity involved obfuscated PowerShell code execution, which is commonly associated with advanced cyber threats.

The Challenge

The client's systems were exhibiting signs of compromise, yet the source of the activity was unclear. The suspicious behavior included:

- Execution of obfuscated Base64-encoded scripts via PowerShell
- Attempts to connect to external repositories (e.g., PasteBin) to retrieve weaponized code

Response Strategy

Avalon initiated a comprehensive digital forensics and incident response (DFIR) investigation, including:

- Threat hunting across affected systems
- Analysis of the cyber kill chain to trace the origin and intent of the attack
- Identification of third-party software involvement

Investigation Findings

The forensic analysis revealed that the suspicious activity originated from a remote support utility – Bomgar – used by a third-party vendor. Although the client did not use Bomgar directly, a vendor employed it to manage on-premise applications.

The forensic analysis revealed that the **suspicious activity originated** from a **remote support utility** used by a **third-party vendor.**

Once access was gained via Bomgar, the attacker:

- Executed obfuscated PowerShell scripts
- Attempted to retrieve malicious payloads from PasteBin
- Aimed to establish a command and control (C2) channel
- Planned to deploy exploitation frameworks such as PowerSploit for lateral movement and data exfiltration

Case Study: Incident Response

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

Containment & Mitigation

Avalon's MDR sensors successfully blocked the malicious activity on systems where they were deployed. However, systems relying solely on traditional antivirus did not detect the threat, prompting a broader investigation.

Using sandbox environments, Avalon confirmed:

- The PasteBin-hosted code was weaponized
- The attacker intended to establish persistent access and deploy additional tools for exploitation

The Outcome

Avalon's swift response and advanced threat detection capabilities:

- Prevented a full-scale breach
- Averted potential data loss, ransomware deployment, and system manipulation
- Highlighted the critical importance of monitoring third-party vendor access

Key Takeaways

- Third-party risk remains a significant threat vector
- Obfuscated scripting and remote access tools are common in modern attack chains
- Proactive MDR and DFIR are essential to detect and neutralize threats before damage occurs

QUESTIONS?

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

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com