Incident Case Study: SharePoint ToolShell Zero-Day Exploitation (CVE-2025-53770)

Overview

This incident involved the successful exploitation of a critical zero-day vulnerability known as **ToolShell (CVE-2025-53770)** targeting an on-premises **Microsoft SharePoint Server**. The attack resulted in **unauthenticated remote code execution (RCE)**, post-exploitation activity, and the establishment of persistence on a production server. The incident was identified and investigated from a Tier-3 SOC perspective, leveraging network, endpoint, and application-layer telemetry.

Detection & Initial Alert

The incident was triggered by a SOC detection rule specifically designed to identify **ToolShell exploitation patterns**, flagging an **unauthenticated HTTP POST request** to the vulnerable endpoint:

```
/_layouts/15/ToolPane.aspx?DisplayMode=Edit
```

The request originated from an external cloud-hosted IP and included a large payload and spoofed headers, consistent with early-stage zero-day exploitation techniques. Proxy logs confirmed the request was **allowed** and successfully reached the SharePoint application.

Attack Analysis

Traffic analysis revealed the source IP belonged to a **cloud hosting provider**, commonly abused for short-lived attack infrastructure. Reputation checks showed partial malicious classification, which—combined with exploit-specific behavior—supported a **true positive determination**.

Post-exploitation investigation uncovered the use of **Living-off-the-Land binaries (LOLBins)** such as `cmd.exe`, `powershell.exe`, and `csc.exe` to execute encoded payloads, compile malicious executables directly on the server, and evade traditional signature-based detection. A decoded PowerShell payload revealed server-side C# code designed to extract **ASP.NET MachineKey cryptographic secrets**, enabling authentication bypass and token forgery.

The attacker then established persistence by writing a **malicious ASPX web shell** into the trusted SharePoint LAYOUTS directory. This web shell facilitated secondary payload delivery from attacker-controlled infrastructure, confirming full system compromise.

Impact Assessment

The compromise posed a **high risk to authentication integrity and data security**, as stolen MachineKeys could be used to forge SharePoint authentication cookies and impersonate users. The presence of a persistent web shell indicated the attacker maintained ongoing access beyond the initial exploit window.

Incident Response Actions

Recommended actions included immediate server isolation, forensic evidence preservation, credential and cryptographic key rotation, removal of malicious artifacts, and a full system rebuild from a known-good backup. Environmental threat hunting was advised to identify any additional affected systems or reuse of indicators.

Conclusion

This incident represents a **confirmed real-world exploitation of a zero-day vulnerability**, progressing through multiple stages of the attack lifecycle: initial access, execution, credential material access, persistence, and payload staging. The investigation highlights the importance of **behavior-based detections, layered telemetry correlation, and rapid response** when dealing with modern fileless and zero-day threats.

Skills Demonstrated

- Tier-3 SOC investigation and incident correlation
- Web application exploit analysis
- Endpoint and network telemetry analysis
- Payload decoding and reverse analysis
- MITRE ATT&CK mapping and kill-chain reconstruction
- Incident response decision-making and documentation