TrustedSec

CASE STUDY

THREAT HUNTING LOG4j

Utilizing a Proven Framework to Uncover Threats From Newly Discovered Vulnerabilities

ENGAGEMENT LEAD

JUSTIN VAICARO

Principal Incident Response Consultant

Vaicaro has served in both the Marine Corps and Air Force and has 20 years of experience within the Information Technology industry, with the last 10+ years solely focused on security engineering. Although Vaicaro has held multiple roles throughout his career, his technical strength is derived from his vast network engineering experience. Vaicaro's current focus is on Security Architecture and Design, Incident Response, Malware Reversing, Threat Hunting, Threat Intelligence, and Security Operations.

On December 09, 2021, a severe vulnerability for Apache Log4j was released (CVE-2021-44228). This vulnerability, also known as Log4Shell, allows remote code execution in many applications through web requests and without authentication. Attackers on the Internet began to scan and exploit this vulnerability almost immediately.

A NEW PROBLEM

After following TrustedSec's Log4j Detection and Response Playbook, an organization was concerned that they might have attackers in their network, as the Log4j vulnerability had been pervasive in their environment. While many attacks are possible with a compromised application, the Log4j vulnerability allows remote code execution without validating the entity's authentication. Once the vulnerability became public, attackers quickly moved to exploit this ubiquitous code, as it exposes nearly every server to ransomware groups and cryptocurrency miners on the Internet.

Additionally, attackers were finding new ways to use this exploit to bypass web application firewall rules and brittle Log4j attack detections. Although several tools were released to identify insecure application code and uncover the presence of the insecure library, identifying and understanding post-exploit payloads and activities often requires a more thorough examination. However, most organizations do not have the resources or expertise to discover these advanced threats.

While the organization was generally concerned about the vulnerability's presence within their network, potential exposure of personally identifiable information (PII) was of particular interest. Their paramount objective was to conclusively determine whether PII had been accessed by attackers who exploited the Log4j vulnerability.

A PROVEN PROCESS

Because many organizations struggle to understand whether a breach is actively in progress or has happened at some point in the past, TrustedSec first searches for evidence of a compromise. The Log4j Threat Hunting exploration included network, endpoint, and cloud infrastructure, investigating anomalies that may have taken place.

While this Threat Hunting engagement was specific to the Log4j vulnerability, it followed a process that TrustedSec utilizes to help organizations search for any kind of malicious activity that evades existing security monitoring, detection, and alerting. If done properly, Threat Hunting can be one of the most effective ways to detect evidence of a compromise, uncover security operation misconfigurations, and identify insecure business process activities. Even though attackers are skilled at bypassing detection devices, their tactics, techniques, and procedures (TTPs) still leave traces of their activity. By searching for these traces within the environment, active or dormant threats can be identified.

TrustedSec's Threat Hunting methodology is built around a loop process consisting of four (4) steps that define an effective detection approach.

First, a hypothesis is created around an activity or specific threat that pertains directly to an organization, its business sector, intellectual property, or geographic location. Next, specific attacker TTPs are investigated to build applicable detection capabilities around the hypothesis.

TrustedSec uses manual techniques, tool-based workflows, and analytics to uncover potential logging visibility gaps throughout the Threat Hunting process. Identification and resolution of these gaps provides assurance that the organization has the detection capabilities necessary to meet the hypothesis requirements. Detection automation and Security Operations Center (SOC) alert tuning are informed and enriched using the data analyzed and information gathered during the Threat Hunting process.

To find out more about TrustedSec's Threat Hunting methodology, read our full Guide To Successful Threat Hunting.

TANGIBLE BENEFITS

After completing the Threat Hunting engagement, it was determined that the Log4j vulnerability had not been exploited within the system, and PII had not been accessed. Definitively confirming this allowed the organization to take the next steps towards remediating the gap and developing plans for handling future exploits.

While there may not have been evidence of an attack within the organization's environment, the peace of mind from that discovery was valuable in itself. Additionally, although the engagement didn't uncover specific issues in the environment, it did present opportunities to harden it.

While this Threat Hunting engagement was performed to identify existing exposure from the Log4j vulnerability, this type of engagement can be used as a proactive measure that organizations can take against any kind of threat. Overall, Threat Hunting increases an organization's ability to uncover security incidents and improve defensive systems.

TrustedSec

877.550.4728
info@TrustedSec.com
TrustedSec.com

TrustedSec is an information security consulting team at the forefront of attack simulations with a focus on strategic risk management. Our goal is to help organizations defend against threats of all kinds and change the security industry for the better.

By investing in exceptional people, TrustedSec enhances client security, elevates the infosec community, and creates a more secure world.