OUTBREAK ALERTS

Lazarus RAT Attack

APT group exploiting Log4j2 vulnerability to deploy Remote Access Trojans (RAT)

https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
CVEs: CVE-2021-44228

A new campaign conducted by the Lazarus Group is seen employing new DLang-based Remote Access Trojans (RATs) malware in the wild. The APT group has been seen to target manufacturing, agricultural and physical security companies by exploiting the Log4j vulnerability and using it for initial access leading to a C2 (command and control) channel with the attacker.

Background

Lazarus is an advanced persistent threat (APT) actor sponsored by the North Korean government. In this particular campaign, Lazarus's initial access begins with successful exploitation of CVE-2021-44228, the infamous Log4j vulnerability discovered in 2021.

Log4Shell is an unauthenticated remote code execution (RCE) flaw that allows taking complete control over systems using vulnerable versions of Log4j library. The flaw was discovered as an actively exploited zero-day on December 10, 2021, and its widespread impact, ease of exploitation, and massive security implications acted as an open invitation to threat actors. To learn more please read the outbreak report:
https://www.fortiguard.com/outbreak-alert/log4j2-vulnerability

Announced

December 11, 2023: Cisco Talos posted a blog and shared latest findings on;
https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram

Fortinet customers remain protected by the IPS signature "Apache.Log4j.Error.Log.Remote.Code.Execution" and the Antivirus detections for the related malware (Lazarus RATs).

Latest Developments

December, 2023: According to the FortiGuard telemetry, there is a significant increased activity in the IPS detection of upto 65,000+ unique IPS devices. However, this particular campaign is just one of the instance where threat actors are still actively targeting the log4j vulnerability and using it as an initial access due to its widespread usage.

According to a report by Veracode, over 30% of Log4J apps still use a vulnerable version of the library after 2 years of the patches being released and a log4j dashboard by Sonatype shows, 25% of the library's downloads in the past week concerning vulnerable versions.
https://www.sonatype.com/resources/log4j-vulnerability-resource-center

FortiGuard Labs recommends companies to scan their environment, find the versions of open-source vulnerable libraries in use, and develop an upgrade plan for them and always follow best practices.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Decoy VM

Detects activities related to the Log4j2 vulnerability

FortiDeceptor
DB 202211105

Weaponization

Delivery

AV

Detects and blocks Remote Access Trojan (RATs) related to the Lazarus RAT Attack

FortiGate *DB 91.09630* | FortiWeb *DB 91.09630* | FortiClient *DB 91.09630* | FortiSASE *DB 91.09630* | FortiMail *DB 91.09630* | FortiCASB *DB 91.09630* | FortiCWP *DB 91.09630* | FortiADC *DB 91.09630* | FortiProxy *DB 91.09630*

Vulnerability

Detects presence of Log4j2 vulnerability

FortiClient *v5.0+*

AV (Pre-filter)

Detects and blocks Remote Access Trojan (RATs) related to the Lazarus RAT Attack

FortiEDR *DB 91.09630* | FortiSandbox *DB 91.09630* | FortiNDR *DB 91.09630*

Exploitation

IPS

Blocks exploitation of the Log4j2 vulnerability

FortiGate *DB 22.404* | FortiSASE *DB 22.404* | FortiNDR *DB 22.404* | FortiADC *DB 22.404* | FortiProxy *DB 22.404*

Web App Security

Blocks exploitation of the Log4j2 vulnerability

FortiWeb *DB 0.00308* | FortiADC *DB 1.00030*

Installation

Post-execution

Detects post-exploitation behavior associated with the Log4j2 vulnerability.

FortiEDR *v5.0+*

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient *DB 1.00017* | FortiAnalyzer *DB 1.00031* | FortiSIEM *DB 602*

Threat Hunting

FortiEDR *v5.0+* | FortiAnalyzer *v6.4+*

Playbook

FortiSOAR *v7.4.+*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training | Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating | FortiDAST

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiDevSec | FortiEDR

Additional Resources

The Hacker News	https://thehackernews.com/2023/12/lazarus-group-using-log4j-exploits-to.html
Dark Reading	https://www.darkreading.com/threat-intelligence/lazarus-group-still-using-log4shell-rats-written-d
Security Week	https://www.securityweek.com/north-korean-hackers-developing-malware-in-dlang-programming-language/
CISA Guidance	https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance

Learn more about FortiGuard Outbreak Alerts