BLACKSWAN CYBERSECURITY

# THREAT ADVISORY

September 16, 2024

## Hadooken Malware Targeting Oracle WebLogic

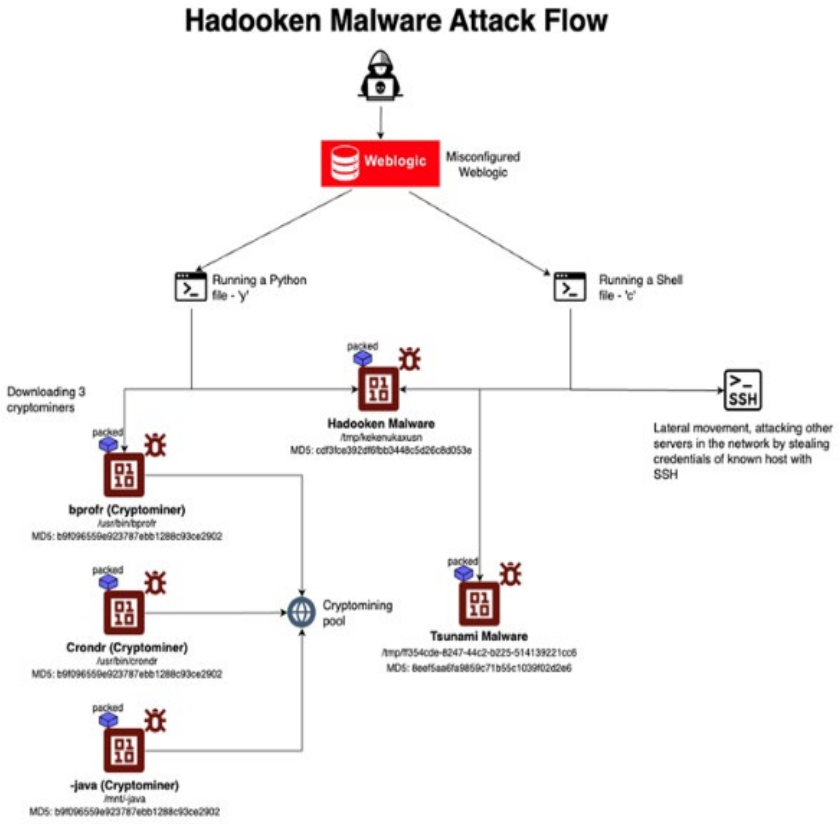
### SUMMARY

A new malware campaign was recently identified that targets Linux environments, focusing on crypto-mining and botnet malware deployment. This operation specifically targets Oracle Weblogic servers to deliver a malware strain called "Hadooken," as reported by cloud security firm Aqua. "When Hadooken is executed, it installs Tsunami malware and deploys a crypto miner."

### TECHNICAL DETAILS

Oracle WebLogic Server is an enterprise-level Java EE application server, widely used for building, deploying, and managing large-scale distributed applications. It is popular in banking, e-commerce, and critical business systems due to its support for Java, transaction management, and scalability. WebLogic is often targeted in cyberattacks, primarily due to vulnerabilities such as deserialization flaws, improper access controls, and common misconfigurations – examples include weak credentials or exposed admin consoles. These weaknesses can lead to severe risks, including remote code execution (RCE), privilege escalation, and data breaches, especially if systems are not properly patched or secured.

The recent attack campaign leverages these vulnerabilities and configuration weaknesses to gain an initial foothold and execute arbitrary code on vulnerable WebLogic instances. The attack begins by deploying two nearly identical payloads: one written in Python and the other as a shell script. These payloads retrieve the "Hadooken" malware from a remote server, with IP addresses "89.185.85[.]102" or "185.174.136[.]204."



The shell script version is designed to search directories containing SSH data, including user credentials and host information using this data to launch attacks on other known servers. This enables lateral movement within the compromised environment, spreading Hadooken malware across the network or connected systems.

Hadooken itself consists of two primary components: a cryptocurrency miner and a distributed denial-of-service (DDoS) botnet named "Tsunami" (also known as Kaiten). Tsunami has previously targeted Jenkins and WebLogic services, especially in Kubernetes environments. Once deployed, Hadooken ensures persistence by creating cron jobs that run the crypto miner at regular intervals.

To evade detection, Hadooken employs various defense evasion techniques. It uses Base64-encoded payloads and disguises malicious processes by naming them innocuously as “bash” or “java” to blend with legitimate system activity. Additionally, it deletes artifacts and traces of its execution to avoid detection. The IP address 89.185.85[.]102 is associated with a hosting provider in Germany, Aeza International LTD (AS210644). A report from Uptycs in February 2024 linked this IP to the "8220 Gang", which exploited vulnerabilities in Apache Log4j and Atlassian Confluence Server and Data Center for cryptocurrency mining. The same infrastructure is now implicated in the Hadooken campaign, reflecting a consistent trend in abusing known enterprise vulnerabilities.

## INDICATORS OF COMPROMISE (IOCs)

**Hashes:**

- cdf3fce392df6fbb3448c5d26c8d053e
- 4a12098c3799ce17d6d59df86ed1a5b6
- b9f096559e923787ebb1288c93ce2902
- 9bea7389b633c331e706995ed4b3999c
- 8eef5aa6fa9859c71b55c1039f02d2e6
- c1897ea9457343bd8e73f98a1d85a38f
- 249871cb1c396241c9fcd0fd8f9ad2ae
- 73d96a4316182cd6417bdab86d4df1f

**Attacker IP:**

- 185.174.136.204
- 89.185.85.102

## RECOMMENDATIONS

- Ensure that Oracle WebLogic servers are consistently updated with the latest security patches to close known vulnerabilities like deserialization flaws.
- Use strong, unique credentials for all admin and user accounts, and disable unnecessary admin interfaces. Implement multi-factor authentication (MFA) where possible.
- Regularly audit server configurations to identify misconfigurations such as exposed admin consoles and weak credentials. Limit access to sensitive areas like SSH directories.
- Set up intrusion detection systems (IDS) to monitor unusual traffic, especially from known malicious IP addresses, such as those linked to the Hadooken campaign.
- Restrict the privileges of user accounts and processes to minimize the impact of potential malware execution.
- Install and maintain anti-malware tools on all systems to detect and block malicious activities, including crypto miners and botnets like Tsunami.
- Automate the process of identifying and mitigating vulnerabilities using tools such as vulnerability scanners and patch management solutions.
- Segment the network to prevent malware from easily moving laterally between systems. Use firewalls and access control lists (ACLs) to enforce boundaries.
- Maintain comprehensive logging of all system and network activities to detect unusual behaviors, such as unauthorized SSH access or cron job creations.

- Ensure regular backups of critical systems and test recovery plans to minimize data loss in the event of a malware attack or breach.

**REFERENCES**


- https://www.aquasec.com/blog/hadooken-malware-targets-weblogic-applications/
- https://thehackernews.com/2024/09/new-linux-malware-campaign-exploits.html