New cryptojacking malware called Pro-Ocean is now attacking Apache, Oracle and Redis servers

seguranca-informatica.pt/new-cryptojacking-malware-called-pro-ocean-is-now-attacking-apache-oracle-and-redis-servers/

February 3, 2021

New cryptojacking malware called Pro-Ocean is now attacking Apache, Oracle and Redis servers.
Security experts from the Unit42 – PaloAlto Networks Team **published** an article describing how a recent malware targeting Apache, Oracle, and Redis servers in the wild. The researchers believed the malware operators are related to the China-based cybercrime group Rocke, a malicious team detected in 2019 for using cloud-targeted malware.

In recent days, security researchers have detected that the financially-motivated Rocke hacking group is using a new piece of Cryptojacking malware named Pro-Ocean to target all the vulnerable servers of Apache ActiveMQ, Oracle WebLogic, and Redis.

The Pro-Ocean Cryptojacking malware is equipped with an advanced rootkit and worm capabilities, also using the most advanced techniques and tactics as a way of bypassing security appliances, EDR and AV.

Modus Operandi

This new piece of malware is using the XMRig miner, which is disreputable for its use in every Cryptojacking operation. Some key point about the malware are:

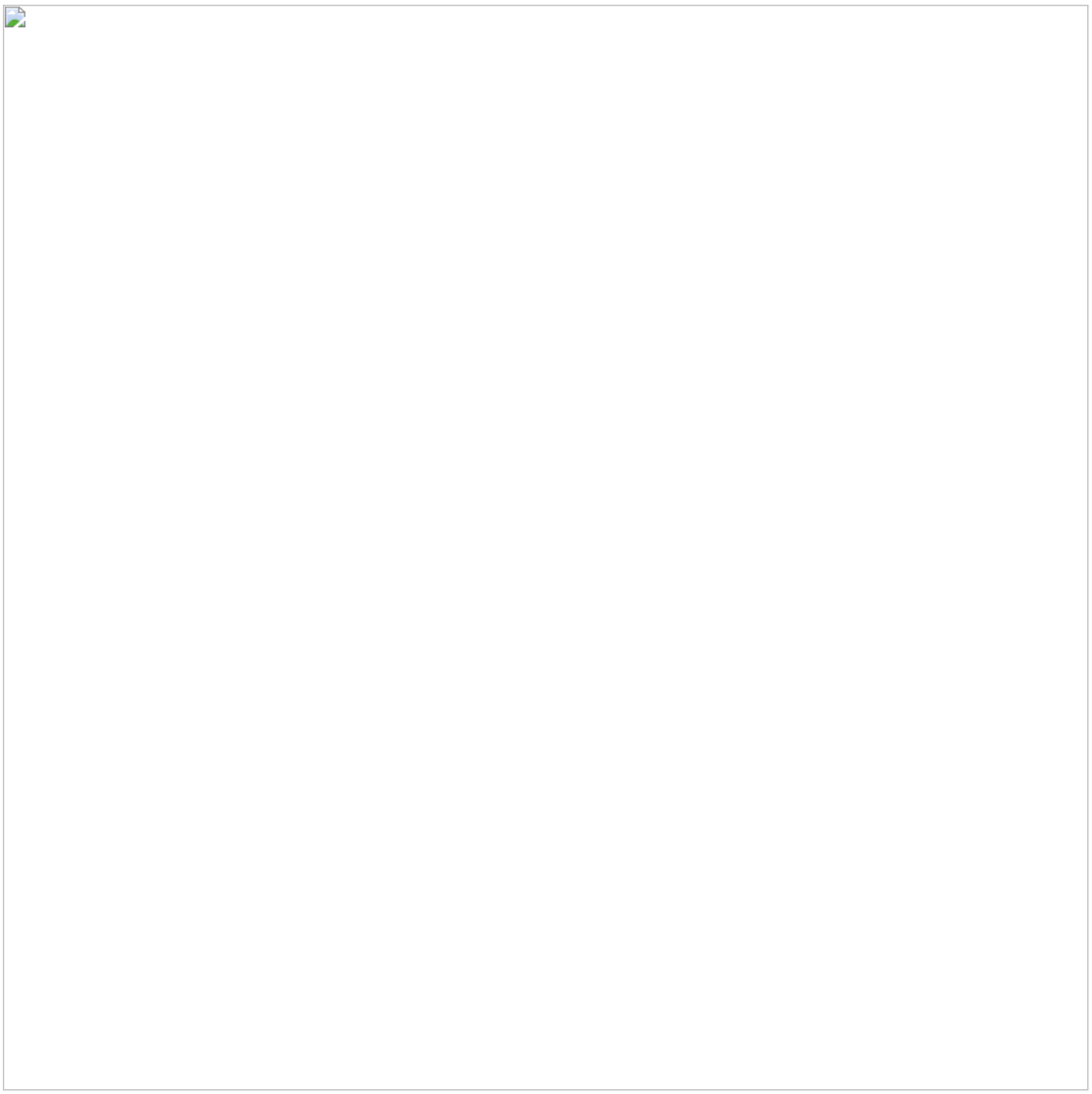
- *The binary is packed using UPX. This means that the actual malware is compressed inside the binary and is extracted and executed during the binary execution.*
- *Advanced static analysis tools can unpack UPX binaries and scan their content. However, in this case, the UPX magic string has been deleted from the binary, and therefore, static analysis tools cannot identify this binary as UPX and unpack it.*
- *The modules are gzipped inside the unpacked binary.*
- *The XMRig binary is inside one of the gzipped modules and is also packed by UPX and does not have the UPX magic string.*

In detail, the Pro-Ocean malware was developed in Go, which is organized with an x64 architecture binary, and it generally targets the typical cloud apps like Apache ActiveMQ, Oracle Weblogic, and Redis.

Modules & Functions

The malware uses four modules of Pro-Ocean, and these modules are gzipped inside the binary and are removed and executed one by one with four different functions.

```
main_ReleaseExe
main_ReleaseExelk
main_ReleaseExerkt
main_ReleaseExescan
```



The Four modules are:

```
Rootkit Module
Mining Module
Watchdog Module
Infection Module
```

List of the vulnerable software

According to the **report**, Pro-Ocean also operates to eliminate opposition by killing other malware and miners, and all these include Luoxk, BillGates, XMRig, and Hashfish, and all these runs on the negotiated host.

In detail, this malware also comes with a watchdog module that is being written in Bash that guarantees endurance and takes care of dismissing all the processes that are being utilized by more than 30% of the CPU with the purpose of mining Monero efficiently.

Apart from this, more information are yet to extract, as the experts are trying to circulate all the necessary details regarding this malware. So, the list of vulnerable software are still not finite; however, this malware is an illustration that demonstrates cloud providers' agent-based security answers.

More details about this threat **here**.

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.