Pro-Ocean

Threat: **Cryptomining Malware**

Author: **Jeffrey Farnan** Date Originally Published: **March 30th, 2021**

1. SUMMARY

Pro-Ocean first spotted in 2019, started out as cryptomining malware, targeting the cloud infrastructure. It targets cloud applications using known vulnerabilities in out of date server packages like ApacheActiveMQ and Oracle WebLogic. A new revised and stealthier version has been seen this year, with added worm and rootkit modules. A new growing trend can be seen of crypto-mining malware becoming a more sophisticated attack.

2. MALWARE FAMILY

- **Type** = Cryptominor.
- **Sub-type** = Worm / Rootkit.

- This type of malware comes from the Crypto-mining family. Crypto-mining is when someone else is using your computer to mine cryptocurrency like Bitcoin or Monero. But instead of cashing in on your own computer's horsepower, the collected coins go into the other person's account and not yours.
- Pro-Ocean attempts to remove other cryptomining malware which may be running on the system, plus it also attempts to kill and high running processes which heavily use the CPU. Once deployed this malware uses XMRig miner 5.11 to mine Monero.
- Pro-Ocean's level of sophistication has increased by adding more modules. To make it stealthier and hide it's activates it has added a rootkit module and a worm module to rapidly spread to other devices on its network.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = China.
- **First seen date/period** = March 2019.
- **Updated version first seen / period** = January 2021.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = February 28th, 2021.

4. MALWARE HISTORY

- The original version of Pro-ocean first seen in 2019, conducted cryptojacking attacks to mind or Monero. The Pro-ocean name came from installation script the attacker chose.
- Pro-ocean Malware comes from the cybercrime gang called the Rocke Group. The Rocke Group first seen in 2018 are known for targeting Linux based cloud infrastructures with cryptojacking attacks.
- Security researchers had Pro-ocean Malware on their radar this last couple of years and so it is well documented. This may have hampered the Rocke Group's cryptojacking operation, which is why we are seeing a new updated and stealthier version of this malware.

5. MALWARE DESCRIPTION

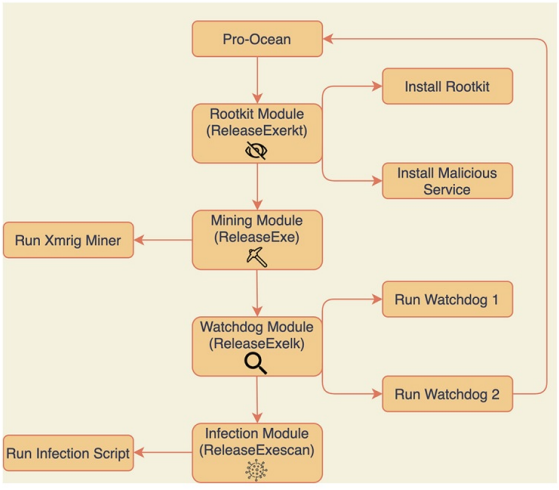
Pro-ocean shows an advanced level of sophistication not seen on the original version of this malware. This shows the cybercriminals are evolving and trying to keep ahead of the cybersecurity companies.

- Pro-Ocean targets known vulnerabilities in cloud applications, such as Apache ActiveMQ, Oracle WebLogic and Redis (unsecure instances).
- One of its first tasks is to uninstall any monitoring agents on the system to avoid detection.
- The second stage is to remove any other malware or cryptomining software on the system. Minors such as Luoxk, BillGates, XMRig and Hashfish.
- The third stage is to install the malware, and kill any high CPU heavily running process on the system.

The Malware: Pro-ocean attempts to disguise itself as benign, but uses several layers of obfuscation. It is packed using UPX and modules are gzipped inside the upacked binary. The UPX magic string which identifies it as packed has been deleted, so static analysis tools cannot identify this binary as UPX and unpacked it.

The Code: The security experts confirm that Pro-ocean is written in Go and each of the four modules of files written in multiple languages (C, Python or Bash) and a bash script that executes it.

Pro-Ocean Malware comprises of four-module structure, consisting of a rootkit module, a mining module, a watchdog module, and an infection module.



- **Rootkit module -**The Pro-Ocean rootkit module is used to hide it malicious activities. It forces binaries to load specific libraries before others, allowing the preloaded libraries to override any function from any library. This way, once executed, binaries will load this library and use its functions instead of the functions in the default libraries. This feature is commonly abused by other malware. Pro-Ocean will try to gain persistence by copying itself into several locations, create malicious services, and execute the malware in case it's not running. What is new is it uses publicly available code, helping to conceal its malicious activity.
- **Mining module** - This module is the main reason Pro-Ocean exists, its main aim is to mine Monero into the attacker's wallet using the XMRig miner 5.11.1.
- **Infection module – (or worm module)** It uses a python infection script to implement its worm capabilities. This script takes the infected machines public IP address using the indent.me service and tries to infect all machines on the same 16-bit subnet. The script runs all of its vulnerability exploits searching for a successful breach of an unpatched version of the ApacheActiveMQ and Oracle WebLogic server software products. If successful, the script delivers a payload to new devices, which downloads and installation script for Pro-Ocean from a remote HTTP server.
- **Watchdog module** – This is the stealthy module, which aim to remove any other miners, malware already running on the system. It uninstalls any monitoring agents that could raise the alarm and deletes firewall iptables. This module also keeps an eye on CPU usage of legitimate running processes, any process running more than 30% it kills it.

6. POTENTIAL CUSTOMER DEFENSE

This malware main target is outdated, internet-connected software like ApacheActiveMQ and Oracle WebLogic, which target exploits found in these server software packages. The first thing to do is keep these software packages up to date, and run periodic updates every so often. Some other measures include the following:

- Use reliable anti-virus software to detect and remove PC threats.
- Check periodically your antivirus has not been removed.
- Check for the sudden removal of high running processes on your server.
- Check your firewall settings and iptaples are still intact.

Research Sources:

- https://www.bleepingcomputer.com/news/security/new-pro-ocean-malware-worms-through-apache-oracle-redis-servers/
- https://www.enigmasoftware.com/prooceanmalware-removal/
- https://www.spywareremove.com/removeprooceanmalware.html
- https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.