Luoxk Malware – Exploiting CVE-2018-2893

By Duncan

Published: 2018-07-27 · Archived: 2026-04-02 10:35:00 UTC

First observed in 2017, Luoxk is a malware campaign targeting web servers throughout Asia, Europe and North America.

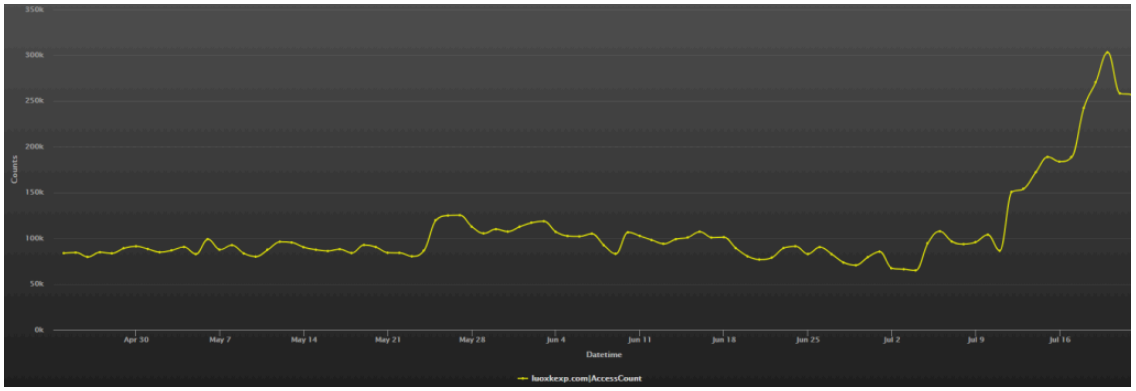
Luoxk uses a variety of methods to compromise vulnerable servers but is primarily exploiting CVE-2018-2893, a remote code execution vulnerability on Oracle web servers. Open Remote Desktop Protocol ports have also been used to infect devices.

The luoxk group registered the luoxkexp[.]com C2 domain on March 16,2017, and then immediately started to use it – domain details here

Once access is achieved, the group operating Luoxk will use the compromised servers for a number of purposes including:

- Enrolling them in a Nitol variant botnet to be used for distributed denial-of-service attacks. Nitol is a smaller botnet trojan that operates primarily in China and surrounding Asian countries.
- Installing the Gh0st remote access trojan, which in turn is used to install an XMRig mining application and to propagate to other devices on the network.
- Hosting malicious Android APK files for other malware to use.

The dns access traffic going to luoxkexp[.]com has been going up for the last few days.



Traffic to luoxkexp[.]com July 2018

Indicators of Compromise

IP Addresses

- 121.18.238[.]56
- 103.99.115[.]220

URLs

- luoxkexp[.]com

Full URL's

http://xmr.luoxkexp.com:8888/xmrig
http://xmr.luoxkexp.com:8888/xmr64.exe
http://xmr.luoxkexp.com:8888/version.txt
http://xmr.luoxkexp.com:8888/jjj.exe
http://xmr.luoxkexp.com:8888/7799
http://xmr.luoxkexp.com:8888/2.exe
http://xmr.luoxkexp.com:8888/1.sh
http://xmr.luoxkexp.com:8888/1.exe
http://xmr.luoxkexp.com/
http://xmr.luoxkexp.com/1.exe
hxxp://103.99.115.220:8080/JexRemoteTools.jar
hxxp://121.18.238.56:8080/aaa.exe
hxxp://121.18.238.56:8080/testshell.sh
hxxp://121.18.238.56:8080/SYN_145
hxxp://121.18.238.56:8080/a4.sh
hxxp://121.18.238.56:8080/SYN_7008
hxxp://121.18.238.56:8080/a5.sh
hxxp://121.18.238.56/xmrig
hxxp://luoxkexp.com:8099/ver1.txt

MD5 File Hashes

- 2f7df3baefb1cdcd7e7de38cc964c9dc

CVE-2018-2893 was addressed in Oracle's July 2018 Critical Patch Update (CPU).

Users are advised to update their affected systems immediately.

Duncan is a technology professional with over 20 years experience of working in various IT roles. He has a interest in cyber security, and has a wide range of other skills in radio, electronics and telecommunications.

Source: https://www.systemtek.co.uk/2018/07/luoxk-malware-exploiting-cve-2018-2893/