Bitcoin Mining Hack 750x7 - Technical Details for Detection and Recovery

Shortcut: If you have been warned specifically about the **IPMI vulnerability** (watch out for the **tag: 750x7ipmi** in the subject),

- your machine(s) has been found by a hacker using metasploit;
- we found his scan results on a hacked machine that we have analysed;
- you can jump directly to **specific notes regarding IPMI.**

Bitcoin Mining Hack "750x7" - Technical Details for Detection & Recovery

Synopsis

Attackers enter linux machines by means of IPMI or RFB console access, install a rootkit and launch a bitcoin miner. Additional functions may include: distribution of hacking/mining software, attacking other machines, possibly stealing passwords.

About this document

This writeup sums up what ACOnet-CERT has learnt during the investigation of an incident. It turned out that many machines were involved, so we set up this page in the hope it will be useful. It aims at helping sysadmins and security teams to

- verify if a machine has been compromised
- assess the impact of the compromise
- recover from the incident.

This writeup refers to one particular campaign, which may or may not correspond to anyones particular situation. Please keep also in mind that the attackers are likely to change their methodology at some point in time, i.e. what's written on this page will become outdated sooner or later. We welcome feedback and updates though (preferably by mail to cert@aco.net).

Distribution on a "need to know" basis is fine with us. It is recommended to simply pass on a link to this page, so that updates can reach the persons involved. Please don't link to this page on a public web site.

Thanks: We would like to thank all those people who have shared their knowledge with us and have provided important hints which helped us a lot in our own work.

Disclaimer: Any information on this page is provided without warranty, may contain errors, misunderstandings and can be misleading, obsolete or otherwise inaccurate. In no way may ACOnet or the University of Vienna be held liable for damages or whatever can cause liability in which jurisdiction ever.

Indicators of Compromise

The following IOCs have been observed on machines involved in the "750x7" hack, but may also be present under other, unrelated circumstances.

Network

- Traffic to 119.78.232.8. This is the bitcoin master server at the time of this writing.
- Inbound ssh connections that can't be attributed to legitimate users.
- Possibly outgoing scanning activity, in particular for port 623 and 5900.
- Possibly outgoing scans for http/htts (port 80/443).

On the backup

With some luck, the backup logs may show when files were created or altered, even if they have been removed since. Things to watch for are e.g.:

- minerd*
- ssh
- ld.so.preload
- _-* (anything that starts with underscore - dash)
- automake, autoconf, ...
- wangyin*

Any findings in the backup log can also help establishing a timeline.

On the machine

Note that the attackers hide their tracks by use of a rootkit. It is recommended to investigate the machine by booting from a know to be safe image, otherwise the output of ps, ls etc. may be misleading. For a quick preliminary check, the rootkit can likely be circumvented by first executing a command like `export LD_PRELOAD=/lib/libc.so.6` (that's on bash, please make sure to point to the correct libc).

- Unexplained reboots.
- rkhunter reporting the libncom rootkit.
- we've heard that /lib/libproc-3.2.8.so has been replaced on some machines, not detected by rkhunter (seen on ubuntu so far, unclear whether other distributions are affected)
- Presence of files in `/tmp` like `do`, `update`, `rc_local_found.`
- Presence of files in /usr/bin like `minerd`, or starting with `_-` (underscore-dash - these should apparently be hidden by the rootkit).
- Presence of `/lib/libncom.*` or `/lib64/libncom.*` and `/etc/ld.so.preload` pointing to this library (beware of the rootkit, see above).
- CPU usage that can't be accounted for. The miner process might only be visible when evading the rootkit (see above).
- CPU usage by processes like metasploit, nmap, minerd.
- Presence of `/usr/local/bin/ssh.`
- Some tools may have been upgraded or installed (gnu auto*, Python, JRE), metasploit, nmap.

Specific notes regarding a possibly vulnerable IPMI interface:

1. A vulnerable machine doesn't necessarily get hacked.
2. The vulnerability, if present, should nevertheless be fixed ASAP.
3. If the interface is exposed to untrusted networks (i.e. the Internet), the attacker we observed would try to access the system
    a. by guessing just a username. This is possible if the so called "cipher 0" is enabled, which implies that no password is required.
    b. to crack the password of an IPMI user after retrieving the Hash. This is possible with weak or moderately complex passwords.
4. However, a cracked password (3b above) may not be exploitable when the user is disabled, the attack would then fail. ACOnet-CERT has no data whether this is the case and can't detect this either, as this would require us to try to attack ourselves.
5. See also the vendor's documentation and make sure the firmware is up to date - see the links below.

Intrusion

As far as we could observe, the attackers intrude the system in one of at least two, possibly three ways:

- IPMI (remote management as in e.g. ILO, DRAC etc, port 623 tcp/udp). The IPMI protocol has severe weaknesses (CERT.cc has a Vulnerability Note specifically about Dell iDRAC) which, if not properly mitigated, would allow an attacker to reboot the machine into a live linux image. He would then mount the root disk, alter it (thereby circumventing any of the target system's security controls), and then reboot the compromised system.
- RFB (remote framebuffer as in e.g. VNC). We currently have no information on how exactly the attackers exploit this protocol, but they are actively scanning for it.
- Possibly by using compromised accounts. We observed that an `ssh` client was dropped in `/usr/local/bin`. Though we haven't analysed it, chances are that this binary collects the user's passwords as they log into other machines from the compromised one.

On the compromised machine, libncom seems to provide access to the attacker. From what we have found about libncom, it hooks some of libc's system calls used by the system's deamons (be it ssh, ftpd, httpd, ...) and immediately opens a (root)shell when the attacker connects. By doing so, the rootkit would bypass any access controls (even tcpwrappers) built into the server, allowing her to get shell access through any service listening to the outside world.

Alterations of the System

The primary goal of the attackers being the bitcoin mining, minerd is downloaded and installed.

To avoid detection, the libncom rootkit is installed. From this point on detection may be difficult, allthough the rootkit doesn't seem to always work properly.

A number of directories and files were touched during installation of various software. Places to look at are /tmp, /usr/bin and /usr/bin, /opt and directories that are seldom looked at by humans eg. /mnt or device directories.

In one case (so far),

- the minerd.gz and some more scripts have been installed in the ftp/http directory.
- metasploit has been used to scan for potential victims.

We are to date not aware of:

- any user accounts being created.
- manipulation of the logfiles.

Remediation

The usual advice is to **disconnect** and then **reinstall** the compromised machine. Considering that a rootkit is used and that the system is manually modified by the attackers, this is probably a good advice.

Be careful to **close the IPMI/RFB-vulnerability** before getting back online, otherwise the attack can be repeated anytime.

Have the users change their **passwords** on the local machine and, if applicable, on machines they connected to via ssh. Be aware that the attackers could also have copied the private **ssh keys**, so these keypairs would need to be replaced as well.

Check for possible lateral movement and intrusions of equally vulnerable servers. Make sure **IPMI/RFB** can't be exploited on any machine.

Countermeasures likely **not to be effective**:

- changing the root password
- using tcpwrappers (hosts.allow / hosts.deny)
- firewalling ssh while leaving any other services accessible

Attribution

None so far.

Deducing the haker's nationality from the network location of the bitcoin master server (China) seems compelling, but may well be completely wrong. During the investigation, we have seen command traffic from several different countries. Any of the machines involved, this also includes the bitcoin master server, may itself have been hacked turning the alleged attacker into the victim. Therefore, we strongly recommend against jumping to conclusions.

Truth is: We don't know who or where the hackers are.

Links and further information

Note that if you use of the tools and information on this page or following any of it's links, you do so at your own risk.

Baseboard Management controllers (BMC) with IPMI:

- Dell iDRAC: Best Practices for Security for iDRAC, IPMI, SNMP
- Dell iDRAC: Vulnerability Note VU#843044 (Dec. 2014)
- Cisco: IPMI Security Vulnerabilities
- Dan Farmer about IPMI security: http://fish2.com/ipmi/
- Metasploit: A Penetration Tester's Guide to IPMI and BMCs
- Article about ipmi vulnerabilities: Many servers expose insecure out-of-band management interfaces to the Internet

Others

- rkhunter (Rootkit detection tool): http://rkhunter.sourceforge.net

Contact and Feedback

ACOnet-CERT welcomes feedback, preferably by e-mail to cert@aco.net. If you are aware of other sites covering this topic, please let us know.

FAQ

Q: Are you saying we have hacked you?

On the contrary! The evidence we found indicates that hackers appear to have your systems on their radar.

Q: I have received a notification from ACOnet-CERT regarding the 750x7 issue. How do you know?

Note: The following applies only if you received a notification by ACOnet-CERT regarding this issue.

We had to analyse a security breach in our constituency (that is: a site was hacked and we looked into it). We found serveral pieces of data with IP addresses. We did our best to interpret these and notify the owners of these addresses. Any background information we can give is on this wiki page.

Q: Can you prove it? Send me logfiles!

Short answer: Sorry, that can't be done.

Long story: As part of handling an incident, we made an effort to

- compile this wiki page,
- interpret the different pieces of evidence we could get hold of,
- try and determine which other systems are involved,
- alert, as a service to the community, the security contacts of these sites.

For us, although we're used to handle these things automatically, it was a large number of contacts. Dealing with gazillions of bounces and autoreplies posed a considerable workload. That said, it was absolutely worth the hassle! Our mission is, after all, to make the internet more secure.

We regret though, that we must decline requests for individual log files or "proof needed by our customer to start the investigation". This would require manual research in every single case – we simply need to protect ourselves from getting overwhelmed, as this would impair our mission. We believe that all the information needed to start the investigation can be found on this wiki page and will be happy to improve it if need be.

Q: Can you check if my site is secure?

Testing for vulnerabilities could arguably be interpreted as hacking. We never launch "hacker tools" against sites outside of our constituency.

Q: What does the name 750x7 stand for?

A.: Nothing in particular. We felt it necessary to clearly distinguish this case/pattern from others like, for instance, the bitcoin mining malware for windows that was found a couple of years ago. Since the attack we investigated had no outstanding characteristics, we couldn't figure out an obvious name. Eventually, we went for an "opaque character string".