HPC-gate

The recent HPC attacks

ICC Theory Lunch
18th May 2019
Alastair Basden

TLP GREEN

National Cyber Security Centre
a part of GCHQ

Alert: Targeting of high-performance computer systems across UK academia

What has happened?

- HPC centres across Europe, US and China have been compromised
  - Unauthorised access
  - Root escalation (in some cases)
    - (a fancy way of saying hackers obtained root access)
    - (so they could then read all files on the system...)
- We *think* COSMA is unaffected
  - But can we really be sure...

Other DiRAC sites

- Cambridge
  - Intrusion but no root escalation (failed attempts)
- Leicester
  - No intrusion
- Edinburgh
  - Intrusion and root escalation
- Durham
  - Attempted intrusion

Timeline

- Monday evening: Cambridge site alerts DiRAC to compromised user, and 2 rogue IP addresses
  - Found 300x a.out processes with a deleted binary under /var/tmp
  - This user is not on Durham
  - No successful logins from these IP addresses
    - Attempted on 23rd April
  - IP addresses blocked (Wuhan and Shanghai)

Late Monday evening

- Becomes apparent that this user was compromised at another site, and attacker achieved root escalation
  - Therefore, all passphrase-less ssh keys on that system should be assumed to be compromised
    - (also ones with a weak passphrase or poor encryption)
  - Initial attack still not understood
  - Several rogue files found:
    - ~/.mozilla/plugins/test, /etc/fonts/.font, /etc/fonts/.low
      - (please check your Linux PCs for these!)
    - Cambridge not affected by these

Tuesday

- Increased list of IP addresses to block
  - Mostly from China
- 2pm – UCL found to be compromised
  - HPC and central Unix service
- Bath compromised (no root escalation)

Late Tuesday

- One exploit identified
  - https://github.com/duasynt/xfrm_poc
    - Adds a user to /etc/sudoers
  - https://duasynt.com/blog/ubuntu-centos-redhat-privesc
- DiRAC-wide ssh key reset discussed

Wednesday

- Some command history discovered (csh)
- Recycling of old keys discussed by DiRAC
  - Old keys to be revoked
  - All keys to be managed within COSMA
    - .ssh/authorized_keys should no longer work
- Archer update issued
  - https://www.archer.ac.uk/status/
  - National Cyber Security Centre become involved
  - Will move to ssh key + password security
  - Archer down all week
- Face-to-face (zoom) DiRAC discussion
- University CIS security office responds
- USA point the blame on China, COVID information theft
  - https://www.us-cert.gov/ncas/current-activity/2020/05/13/cisa-fbi-joint-announcement-prc-targeting-covid-19-research
- Multiple sites known to be compromised
- Initial tip-off to Cambridge from Archer

Official website of the Department of Homeland Security

About Us | Alerts and Tips | Resources | Industrial Control Systems

National Cyber Awareness System > Current Activity Landing
> CISA-FBI Joint Announcement on PRC Targeting of COVID-19 Research Organizations

CISA-FBI Joint Announcement on PRC Targeting of COVID-19 Research Organizations

Original release date: May 13, 2020

Print | Tweet | Send | Share

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have jointly released a Public Service Announcement on the People's Republic of China's targeting of COVID-19 research organizations. CISA and FBI encourage COVID-19 research organizations to review and apply the announcement's recommended mitigations to prevent surreptitious review or theft of COVID-19-related material.

For more information on Chinese malicious cyber activity, see https://www.us-cert.gov/china.

Thursday

- JANET CSIRT team (security) involved and coordinating
  - Zoom meeting called (4pm)
- Appears to be a vulnerability patched in November
  - We applied during February downtime
- COSMA clears out old ssh keys
  - Sparks an avalanche of requests!
  - 15:30-21:30 – SAFE not sending new requests!
- DiRAC@Leicester and Cambridge reset ssh keys
  - DiRAC@Edinburgh is down for hardware repair, and will request when back in production
  -

Friday

- Tesseract identified as compromised
  - (DiRAC@Edinburgh)
  - Announce key/password reset
- HPC Midlands+ Tier 2 also compromised
- Cambridge first compromised in December!
- Newly formed Durham HPC security council meet
  - Hamilton decides on ssh key and password reset
- DiRAC Technical Working Group meet and formulate plan for future action
  - Site-wide trials of 2FA to be recommended
- CSIRT update – initial intrusion believed to be solely due to compromised SSH keys
  - Root escalation method unknown
  - Potentially for crypto currency mining
    - (though others suspect this may be a cover)

Saturday

- DiRAC provide a global list of ssh keys to revoke
  - Applied on COSMA on Monday
  - Some people will need to upload a new key
    - (sorry!)

NIST

NVD MEN

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

https://nvd.nist.gov/vuln/detail/CVE-2019-15239

CVE-2019-15239 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attacker can trigger multiple use-after-free conditions.

QUICK INFO

CVE Dictionary Entry:
CVE-2019-15239
NVD Published Date:
08/20/2019
NVD Last Modified:
09/24/2019

https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

Academic data centers abused for crypto currency mining

[TLP:GREEN]

This page covers ongoing attacks and may be updated (latest: 2020-05-14 16:00:00).

EGI and its supporting organisations deeply care about their international partners and peer infrastructures, and although so far there is no operational impact on EGI, the EGI CSIRT strongly believes in protecting the community and is actively supporting and coordinating the response to the current security incidents affecting the academic and research sector.

Summary

A malicious group is currently targeting academic data centers for CPU mining purposes.
The attacker is hoping from one victim to another using compromised SSH credentials.

The compromised hosts are turned into different roles, including:

- **XMR mining hosts (running a hidden XMR binary)**
- **XMR-proxy hosts** ; The attacker uses these hosts from the XMR mining hosts, to connect to other XMR-proxy hosts and eventually to the actual mining server.
- **SOCKS proxy hosts (running a microSOCKS instance on a high port)** ; The attacker connects to these hosts via SSH, often from Tor. MicroSOCKS is used from Tor as well.
- **Tunnel hosts (SSH tunneling)** ; The attacker connects via SSH (compromised account) and configure NAT PREROUTING (typically to access private IP spaces).

Key points:

- Connections to the SOCKS proxy hosts are typically done via TOR or compromised hosts.
- The attackers uses different techniques to hide the malicious activity, including a malicious Linux Kernel Module (https://github.com/m0nad/Diamorphine).
- It is not fully understood how SSH credentials are stolen.
- At least in one case, the malicious XMR activity is configured (CRON) to operate only during night times to avoid detection.

DiRAC mitigations

- Replace all SSH keys
  - (sorry – that was a pain!)
- Ongoing discussions
  - Bring in ssh key + password
    - Interim, at some sites
  - Eventually bring in 2 factor authentication (2FA)

2FA

- Access given based on something you know and something you have.
  - And which can’t be obtained from a single hacked machine/laptop/PC
- Start with an ssh key
  - Hopefully this will have a passphrase
  - But if your laptop is hacked, a keylogger could obtain the passphrase and the key.
  - Likewise if we force ssh key + password access
- A second device is required
  - To generate a one-time-password

One-time-password

- Second device is typically a smart phone
  - An app is registered with your account
    - A key is provided by COSMA during registration
  - When time to log in, the phone app generates a one-time-password (time limited)
    - Based on current time, and the key
  - You then enter this into COSMA (which also knows current time and the key)
    - Which has also generated the same one-time-password
- Typically valid only for a minute or so
- So only at risk from a key logger for this period.
  - (there are other ways of doing it, but this is most likely to be accepted by DiRAC)

Things to note

- Protect your ssh key
  - Think about where it is backed up to
    - The cloud?
  - Make sure it has a passphrase
    - Use an agent (eg keychain) if you don’t want to enter it every time
    - Use a strong password
- All this seems to have originated from an unprotected ssh key!
- If you updated your key on Thursday, you may need to do so again
  - DiRAC have provided a global list of keys to revoke… (sorry!)