Supercomputers all across Europe have been infected with cryptocurrency mining malware, leading to a number of shutdowns during the crucial period where such machines should be dedicated to research on the coronavirus (aka Covid-19) pandemic.

EPSRC
Engineering and Physical Sciences Research Council
archer
CRAY
NATURAL ENVIRONMENT RESEARCH
ER COMPANY

Security incidents come from all over the continent, including the UK, Germany, Switzerland and, at least rumours insist, Spain. According to a ZDNet report, the first supercomputer to be affected by the malware is the ARCHER system at the University of Edinburgh. The organisation shut down the ARCHER system following a "security exploitation on the ARCHER login nodes," before resetting SSH passwords to prevent further intrusion.

Next up was a report from the bwHPC, the organisation coordinating research projects across the state of Baden-Württemberg, Germany. The organisation admitted it had to shut down five high-performance computing clusters-- namely the Hawk supercomputer at the High-Performance Computing Center Stuttgart (HLRS) at the University of Stuttgart, the bwUniCluster 2.0 and ForHLR II clusters at the Karlsruhe Institute of Technology (KIT), the bwForCluster JUSTUS chemistry and quantum science supercomputer at the Ulm University and the bwForCluster BinAC bioinformatics supercomputer at the Tübingen University-- due to "security incidents."

A day later, security researcher Felix von Leitner published a blog stating a supercomputer in Barcelona, Spain was shut down due to a security issue, while the Leibniz Computing Center (LRZ) under the Bavarian Academy of Sciences disconnected a computing cluster following security breach. Further reports come from Germany, specifically the town of Julich, where the JURECA, JUDAC and JUWELS supercomputers were shut down due to "IT security incident, the city of Dresden, whose Technical University shut down the Taurus supercomputer, and Munich, where a high-performance computing cluster at the Faculty of Physics at the Ludwig-Maximilians University was infected by malware. A final report (at least so far) involves the Swiss Center of Scientific Computations (CSCS) in Zurich, who shut down external access to its supercomputer infrastructure following a "cyber-incident."

The aforementioned organisations failed to publish details on the attacks, but the Computer Security Incident Response Team (CSIRT) at the European Grid Infrastructure (EGI), the pan-European organisation coordinating research on European supercomputers, published malware samples and network compromise indicators from some of the incidents. According to UK-based security firm Cado Security the attackers managed to gain access to the supercomputer clusters via compromised SSH credentials possibly stolen from university members. As for what the attacks involved, the hackers seem to have used an exploit for the CVE-2019-15666 vulnerability to gain root access and install an application mining the Monero (XMR) cryptocurrency.

So far the supercomputers appear to be still shut down in order to resolve the situation.

Go Supercomputers Hacked Across Europe to Mine Cryptocurrency (ZDNet)