Operational security, threat intelligence & distributed computing: the WLCG Security Operations Center Working Group

CHEP 2018 - EPJ Web of Conferences 214, 03029 (2019)
https://doi.org/10.1051/epjconf/201921403029

David Crooks[1*], Liviu Vâlsan[2**], Kashif Mohammad[3***], Shawn McKee[4****], Paul Clark[5†], Adam Boutcher[5‡], Adam Padée[6§], Michał Wójcik[6¶], Henryk Giemza[6‖] and Bas Kreukniet[7**] on behalf of the WLCG Security Operations Center Working Group

[1] STFC Rutherford Appleton Laboratory, Harwell Campus, Didcot, Oxfordshire OX11 0QX, United Kingdom

[2] CERN, The European Organisation for Nuclear Research, 1211 Geneva 23, Switzerland

[3] University of Oxford, Department of Physics, Denys Wilkinson Building, Keble Road, Oxford, OX1 3RH, United Kingdom

[4] Physics Department, University of Michigan, Ann Arbor, MI 48109-1040, USA

[5] Institute for Particle Physics Phenomenology, Ogden Centre for Fundamental Physics, Department of Physics, University of Durham, Science Laboratories, South Rd, Durham DH1 3LE, United Kingdom

[6] Narodowe Centrum Badań Jądrowych, ul. Andrzeja Sołtana 7, 05-400 Otwock-Świerk, Poland

[7] SURFsara, SURF Science Park Building, Science Park 140, 1098 XG, Amsterdam, The Netherlands

3.4 Associated work

The Durham site presented on their work on a distributed Fail2Ban[13] configuration, describing a set of jails which would increase the length of time a particular IP would be banned based on how persistent the activity was.

The Institute for Particle Physics Phenomenology (IPPP) based out of the University of Durham is currently investigating pre-emptive threat blocking across its public facing GridPP High Performance Computing (HPC) cluster using a customised Fail2Ban framework. The framework is used to counter unauthorised access, brute force and denial of service attacks across the site by making use of a shared resource pool of known IP addresses that are believed to be used for such attacks.

To accomplish this the system makes use of a series of nodes running the Fail2Ban client with a number of custom jails and actions to push and pull recent attack data from a shared database. When Fail2ban encounters a threat that IP address is blocked and the information pushed to the database where it is disseminated throughout the site. This halts the attackers progress in moving from system to system to attempt the same attack with the hope of gaining a successful login. This continuous delay slows the attacker down enough that they will hopefully give up and allow enough time for site admins to be alerted to the unauthorised access attempts so further actions can be taken.

To reduce the chances of permanently blocking out entire addresses ranges from known sources each block hit enters a low level jail for a certain period of time. The more hits against this IP, the more it is elevated to a more severe jail until it is finally put into a permanent ban list, requiring an administrator action for removal. In the near future it is hoped this system will be integrated to work with the Malware Information Sharing Platform (MISP) to pull down known Indicators of Compromise and to push any confirmed malicious IP addresses that may be useful to other sites. To increase the data gathering ability of the system, it will also be adapted to make use of target data gathered by remote honeypot systems that will be implemented at a later date. It is hoped that once full implementation is accomplished the system will be capable of performing highly automated defensive actions, making use of an open source, easy to manage framework that can be integrated into other environments with little to no issues occurring.