

Kaspersky Lab and Emerging Threats Pro Partnership to deliver better protection for all

MOSCOW, RUSSIA: Kaspersky Lab, a leading developer of secure content and threat management solutions, has announced its collaboration with Emerging Threats Pro.



Emerging Threats Pro produces a professional grade IDS and IPS ruleset for Snort and Suricata based on and supporting the Emerging Threats open source project. The ruleset focuses on malware and major vulnerabilities, but also provides known bad IP lists and IP/DNS reputation feeds. Kaspersky Lab uses this ruleset for its in-lab internal research work.

The cooperation between the two companies entails collaboration on a malware samples exchange and also combined work on extending Emerging Threats Pro ruleset coverage. Kaspersky Lab's specialists have already begun feeding data into Emerging Threats Pro in order to improve the ruleset for all its users and thus ultimately make the Internet a safer place.

Producing synergies

Commenting on the collaboration, Nikita Shvetsov, director of Anti-Malware Research at Kaspersky Lab, said: "We are happy to be collaborating with the Emerging Threats Pro Team - the open source team to go to for the best IDS/IPS ruleset. Our combined efforts will produce expertise synergies for both organisations to optimise our signatures, which will then trickle down to better Internet security for all."

Matt Jonkman, CEO of Emerging Threats Pro, added: "Our team is excited about the collaboration with Kaspersky Lab. The IDS and anti-virus industries are fighting the same battle, so working closely together as non-competitive companies only makes sense - to strengthen both our organisations' expertise and offerings."

Emerging Threats Pro

Emerging Threats Pro was born out of demand from existing users of the Emerging Threats.net open source rules who wanted a comprehensive enterprise grade IDS/IPS ruleset with a strong malware focus. Its team of researchers and developers has been drawn from among the brightest minds in the open source community, with whose support it is able to produce the fastest moving and most diverse Suricata and Snort rulesets and IP/DNS reputation feeds available.