# Kaspersky Lab’s GReAT Team recognized for ShadowPad discovery

The Kaspersky Lab Global Research and Analysis Team (GReAT) was recognized with the Annual Péter Szőr Award for Technical Security Research for its work on uncovering and analyzing the ShadowPad operation, one of the most significant supply-chain attacks known to date. The award was received at Virus Bulletin 2018, which took place on October 3 through October 5 at the Fairmont Queen Elizabeth hotel in Montreal, Quebec, Canada.

In July 2017, Kaspersky Lab researchers discovered ShadowPad, a backdoor hidden inside server management software that is used by hundreds of enterprises around the world. The malicious code was planted in the latest updates of this software, which is used in industries like financial services, education, telecoms, manufacturing, energy and transportation.

Kaspersky Lab GReAT researchers found that following the installation of an infected software update, the malicious module would send DNS-queries to specific domains (its command and control server) at a frequency of once every eight hours. The request would contain basic information about the victim’s system. If the attackers considered the system to be ‘interesting,’ the command server would reply and activate a fully-fledged backdoor platform that would silently deploy itself inside the attacked computer. After that, on command from the attackers, the backdoor platform would be able to download and execute further malicious code. The threat actor behind the attack is believed to be Chinese-speaking.

“As the widely reported story of ‘NotPetya’ and ‘CCleaner’ show, supply chain attacks are a huge problem. ShadowPad emphasizes the point that such attacks can be very subtle and remain active for a very long time,” said Martijn Grooten, editor, Virus Bulletin. “Kaspersky Lab’s analysis provided both a general overview and very technical details of the attack, which will hopefully lead to more awareness of this threat and the issue of supply-chain attacks in general.”

The Péter Szőr award aims to recognize the best piece of technical security research published each year. Virus Bulletin created the award in Szőr’s honor after the researcher and Virus Bulletin advisory board member passed away in November 2013. Nominations for the award are sought from the security community at large, and a final shortlist is voted on by the Virus Bulletin advisory board. The award is presented each year at the annual Virus Bulletin conference.

“ShadowPad is a prime example of how dangerous and wide-scale a successful supply-chain attack can be. Had it not been detected and patched so quickly, ShadowPad could have affected thousands of organizations worldwide,” said Costin Raiu, director, GReAT. “Receiving the Péter Szőr award at Virus Bulletin is an absolute honor, and we are grateful not only for the recognition, but for the opportunity to continue protecting the world from cybercrime.”

The findings were published on August 15, 2017, and the full report can be accessed on Securelist.com.