



*Issued 6/21/18*

## **Olympic Hackers May Be Attacking Chemical Warfare Prevention Labs**

The team behind the 2018 Winter Olympics hack is still active, according to security researchers -- in fact, it's switching to more serious targets. Kaspersky has discovered that the group, nicknamed Olympic Destroyer, has been launching email phishing attacks against biochemical warfare prevention labs in Europe and Ukraine as well as financial organizations in Russia. The methodology is extremely familiar, including the same rogue macros embedded in decoy documents as well as extensive efforts to avoid typical detection methods. Most of the lab targets were people associated with an upcoming biochemical threat conference run by Spiez Laboratory, which just happened to be involved in the investigation of the nerve agent poisoning of former Russian double agent Sergei Skripal and his daughter Yulia. Also, Kaspersky noted that the custom images and messages in the documents were in "perfect" Russian, and one of them specifically references the Skripal attack. It's generally accepted that Russia tried to frame North Korea for the Olympic hack. It's entirely possible that the Russian targets amounted to a false flag meant to cast doubt on the true origins of the attack. The focus on labs and the Skripal connection may have been meant to rattle the West for daring to attribute assassination attempts to Russia.