

# Operation “Ke3chang”: Targeted attacks against ministries of foreign affairs

 [mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)



## Report

Diplomatic missions, including ministries of foreign affairs (MFA), are high-priority targets for today’s cyber spies. Large-scale cyber espionage campaigns such as “GhostNet” have demonstrated that government agencies around the world, including embassies, are vulnerable to targeted cyber attacks.

As the crisis in Syria escalated in 2013, FireEye researchers discovered a cyber espionage campaign, which we called “Ke3chang,” that falsely advertised information updates about the ongoing crisis to compromise MFA networks in Europe.

We believe that the Ke3chang attackers operated out of China and had been active since at least 2010. However, we believe specific Syria-themed attacks against MFAs (codenamed by Ke3chang as “moviestar”) began only in August 2013. The timing of the attacks precedes a G20 meeting held in Russia that focused on the crisis in Syria.

Download this paper for insight into how ministries of foreign affairs in Europe were targeted and compromised by a threat actor FireEye has dubbed “Ke3chang”.

[Download Now](#)