Mofang: A politically motivated information stealing adversary

blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/

June 15, 2016

Mofang (模仿, Mófa ˇng, to imitate) is a threat actor that almost certainly operates out of China and is probably government-affiliated. It is highly likely that Mofang's targets are selected based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence. This is most clearly the case in a campaign focusing on government and critical infrastructure of Myanmar that is described in this report. Chances are about even, though, that Mofang is a relevant threat actor to any organization that invests in Myanmar or is otherwise politically involved. In addition to the campaign in Myanmar, Mofang has been observed to attack targets across multiple sectors (government, military, critical infrastructure and the automotive and weapon industries) in multiple countries.

The following countries have, in the above named sectors, been affected, although Fox-IT suspects there to be more: India, Germany, United States, Canada, Singapore, South Korea.

Despite its diverse set of targets Mofang is probably one group. This is based on the fact that its tools (ShimRat and ShimRatReporter) are not widely used, and that campaigns are not usually observed in parallel. Technically, the group uses distinct tools that date back to at least February 2012: ShimRat and ShimRatReporter. The mofang group does not use exploits to infect targets, they rely on social engineering and their attacks are carried out in three stages:

1. Compromise for reconnaissance, aiming to extract key information about the target infrastructure.
2. Faux infrastructure setup, designed to avoid attracting attention.
3. The main compromise, to carry out actions on the objective.

The name ShimRat is based on how its persistence is build up. It uses the so-called shims in Windows to become persistent. Shims are simply hot patching processes on the fly, to ensure backward compatibility of software on the Microsoft Windows platform.

As far as known, the only exploits the Mofang group uses are privilege elevation exploits built into their own malware. The vulnerabilities that were being exploited were already known about at the time of use. The full report contains contextual as well as technical information about the group and its activities. These can be used, for example, for threat assessments, compromise assessments, incident response and forensics activities.

> **Download 'Mofang – a politically motivated information stealing adversary'**