MAGIC KITTEN – The Oldest Kitten – ICNA

By ICNA

Published: 2022-04-17 · Archived: 2026-04-05 13:51:09 UTC

In January 2015, the German news outlet Der Spiegel released previously unpublished documents on cyber espionage conducted by American intelligence agencies. One of them revealed an NSA tactic labeled “fourth party collection,” which is the practice of breaking into the command and control infrastructure of foreign-state-sponsored hackers to look over their shoulders. The presentation describes a real-life example of acquiring intelligence and stealing victims from a group code-named VOYEUR by the NSA, otherwise known as Magic Kitten.

Magic Kitten appears to be among the oldest and most elaborate threat actors originating in Iran. It is also distinct from other groups because of its apparent relationship with the Iranian Ministry of Intelligence rather than the IRGC. However, Magic Kitten’s activities mirror those of other groups, with the primary targets being Iranians inside Iran and regional rivals. The earliest observed samples of Magic Kitten’s custom malware agent dates to 2007, well before other known malware apparently originated, and the threat actor continues to be active.

Magic Kitten appears to exercise the most mature tradecraft of Iran-based threat actors. It has opportunistically compromised dozens of websites at random (including those of an Indian hospital, an Italian architect, and a well-

known Canadian comedian) to create a relay network to hide its operations. Such attention to tradecraft appears elsewhere in Magic Kitten's operations, including in the design of malware, which is modular in nature.

Magic Kitten has not been observed using sophisticated exploits and instead appears to rely on social engineering and other common tactics to deceive users. In the case of the journalist Vahid Pour Ostad, the malware was sent by his former Ministry of Intelligence interrogator with a threat attached and relied on private records that would have been available only to government actors. This coordination represents both independent confirmation of the NSA's attribution and an extreme example of the strategies employed by Magic Kitten. Other samples of the malware agent appear to have been delivered posing as Turkish asylum forums for Syrian refugees.

The NSA presentation also provides a window on Magic Kitten's targets up to May 2011, portraying an operation focused on North America, Europe, and the Middle East. These campaigns continued through the June 2013 presidential election of Hassan Rouhani, provoking a blogpost from Google about related attacks.51 As the election approached, exposed logs showed the daily capture of dozens of accounts connected to Iranian cultural and media figures, graduate students, and social activists (including individuals that would later join the Rouhani administration). Magic Kitten continued to target Iranians after the election, attempting to unmask pseudonymous internet users by baiting them with content on women's rights and the security establishment.

Like other Iranian operations, Magic Kitten maintains a strong secondary interest in conducting espionage against regional targets and international foreign policy institutions. CrowdStrike, another American cybersecurity company, accounts for part of this focus on "international corporations, mainly in the technology sector" and other political targets. An NSA slide with a victim map portrays a broad-reaching operation targeting nearly every country in the Middle East. Sinkhole data collected from expired domains previously used as relays and other fallback infrastructure suggest that Magic Kitten, or the malware agent used, continues to actively compromise individuals in Germany, Indonesia, Iraq, Lebanon, the Netherlands, Palestine, Pakistan, Qatar, Sweden, Switzerland, Thailand, and the United Arab Emirates. Notably, compromised individuals in Iraq were also typically in Iraqi Kurdistan, mirroring a common pattern with other threat actors.

A diagram within the NSA presentation suggests that the malware agent employed by Magic Kitten was also used at the time by Hezbollah, under independent infrastructure. While Hezbollah has been known to maintain its own offensive cyber operations and engage in intelligence sharing with Iran, there has been little prior evidence of direct sharing of tools.

[For more on APT read our Hacker series]