Ali Baba, the APT group from the Middle East

By Pierluigi Paganini

Published: 2015-02-17 · Archived: 2026-04-05 17:03:08 UTC

Pierluigi Paganini February 17, 2015

Adrian Nish of BAE System presented the results of its investigation on the Ali Baba APT group operating from the Middle East that hit Western companies.

Yesterday the Kaspersky Lab team revealed the results of its investigation on the hacking crew dubbed the Equation group, a team of hackers that demonstrate extraordinary capabilities and sophisticated tactics, techniques, and procedures. Unfortunately, the number of ATPs is growing over the years, the majority of them goes under the radar for a long period.

In 2013, Adrian Nish of BAE Systems investigated on a cyber attack suffered by an engineering company in the UK that operates in the national power industry. The security experts discovered that hackers have compromised the company network for some time, exfiltrating any kind of information.

> *"The group has probably been working for about two years now," Nish explained. "It's an emerging trend in the Middle East. That's a complicated region and the offensive side of things is becoming complicated there too. There's offensive cyber companies and local malware authoring now."*

Nish identified the C&C servers used by the threat actors and discovered that Google was indexing some of the machines used by the hackers to siphon data. According to the researcher, the bad actors could be members of a pro-Iranian group and proved to have access to a wide set of hacking tools.

BAE firm dubbed the APT group Ali Baba because a code name in one of the tools belonging to their arsenal.

> *"They had taken network diagrams, usernames and credentials from an Israeli university and even an entire Web app that they stole from a group in the Middle East," Nish said in a talk at the Kaspersky Lab Security Analyst Summit here Monday. "They had even stolen some signatures, physical signatures from people who had scanned them for some reason. What could possibly go wrong with that?"*

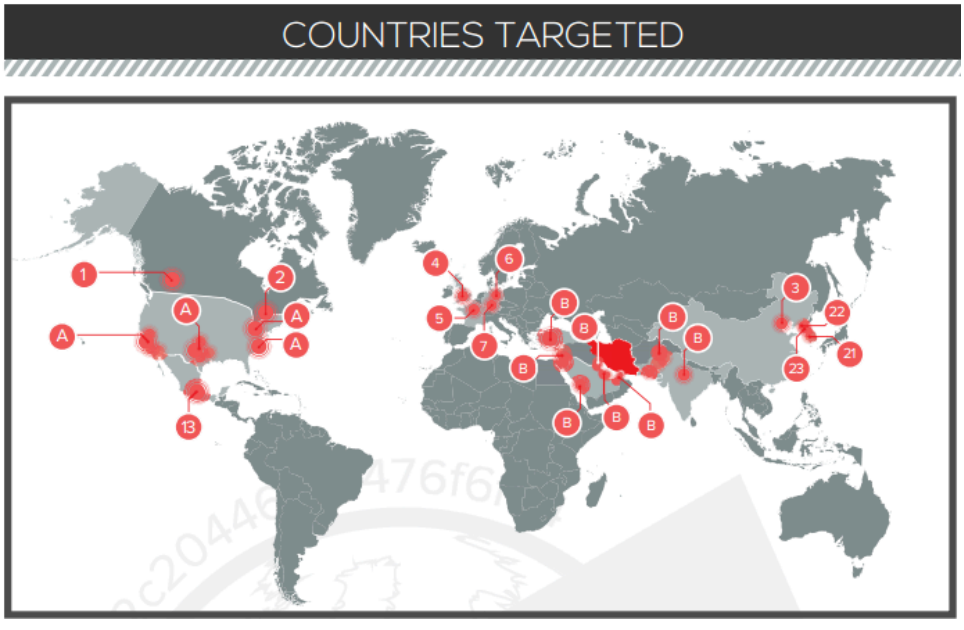
Nish confirmed to have discovered nearly 40 distinct hacking tools, including five modules of custom malware, a key logger, a custom hash cracker and many others. The expert highlighted some interesting methods for defeating incident response on compromised networks and for data exfiltration.

Nish detailed one of the tools in the arsenal of the Ali Baba APT, Fakeddos.exe, that was used the hackers to generate large amounts of junk traffic on compromised networks, a tactic used by the threat actor to overwrite the logs of legitimate traffic making difficult investigation from security firms.

> *"That really makes incident response quite a pain, really," Nish said.*

Ali Baba hackers used a singular exfiltration technique based on email, they disguised the outbound emails as Viagra spam messages to avoid detection of defense systems.

According to a report published by the security company Cylance, the UK firm wasn't the unique known victim of the Ali Baba, the APT also had compromised transportation companies in South Korea and Pakistan. Cylance identified the hacking team as OpCleaver.



Pierluigi Paganini

(Security Affairs – Ali Baba APT, cyber espionage)
