The Gaza cybergang and its SneakyPastes campaign

By Kaspersky Team

Published: 2019-04-10 · Archived: 2026-04-05 14:51:12 UTC

At our Kaspersky Security Analyst Summit (SAS) conference we traditionally speak about APT attacks: It was there that we first published info about Slingshot, Carbanak, and Careto. Targeted attacks are running as high as ever, and this year was no exception: At SAS 2019 in Singapore we spoke about an APT criminal group called the Gaza cybergang.

Rich armory

The Gaza cybergang specializes in cyberespionage, with its campaign mostly limited to the Middle East and countries in central Asia. At the center of its focus are politicians, diplomats, journalists, activists, and the region's other politically active citizens.

In terms of the number of attacks we registered from January 2018 through January 2019, the targets located within the Palestinian territories were very comfortably in the lead. Quite a few infection attempts also fell on Jordan, Israel, and Lebanon. In its attacks, the gang uses methods and tools of varying complexity degrees.

Our experts have identified three subgroups in the cybergang. We have already covered two of those. One was the author of the Desert Falcons campaign, and the other was behind the tailored attacks known as Operation Parliament.

Now it's time to talk about the third, which we call MoleRATs. The group is armed with relatively simple tools, but that doesn't make its SneakyPastes campaign (named for its active use of pastebin.com) less dangerous.

SneakyPastes

The campaign is multistage. It begins with phishing, using letters from one-time addresses and one-time domains. Sometimes the letters contain links to malware or infected attachments. If the victim executes the attached file (or follows the link), their device receives Stage One malware programmed to activate the infection chain.

The letters, meant to quiet the reader's vigilance, are mostly about politics. They are either records of political negotiations or addresses from some credible organizations.

Once Stage One malware is safely onboard the computer, it tries to secure its position, conceal its presence from any antivirus products, and hide the command server.

The attackers use public services (pastebin.com, github.com, mailimg.com, upload.cat, dev-point.com, and pomf.cat) for subsequent stages of the attack (including malware delivery) and, most important, for communication with the command server. Typically, they use several methods simultaneously to deliver the extracted information.

Finally, the device gets infected with RAT malware, which offers powerful capabilities. Among other things, it can freely download and upload files, launch applications, search for documents, and encrypt information.

The malware scans the victim's computer to locate all PDF, DOC, DOCX, and XLSX files, saves them to temporary file folders, classifies, archives, and encrypts them, and finally sends them to a command server via a chain of domains.

In fact, we detect multiple tools used in this kind of attack. You can learn more about them and get more technical details from this post on Securelist.

Integrated protection against integrated threats

Our products are made to successfully combat the components used in the SneakyPastes campaign. To avoid being among its victims, follow these tips.

- Teach your employees to recognize dangerous letters, both mass and targeted ones; Gaza cybergang attacks begin with phishing. Our interactive Kaspersky ASAP platform not only provides that information but also imparts the necessary skills.
- Use integrated solutions built to stand up to complex and multistage attacks that may be too tough for basic antivirus products. To resist attacks at the network level, we recommend a bundle consisting of Kaspersky Anti Targeted Attack and Kaspersky Endpoint Detection and Response.
- If your company employs a dedicated information security service, we recommend you subscribe to Kaspersky Lab's closed reports, where we give detailed accounts of current cyberthreats. You can purchase a subscription by writing to intelreports@kaspersky.com

---