MITRE-ID: G0021

Name: Molerats

Country: Middle East

Description:

Molerats is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States.

TTPs:

Initial Access:

* The group has sent phishing emails with malicious links included.
* The thread actors obtained a list of active processes on the victim and sent them to C2 servers.

Execution:

* The group has sent malicious links via email trick users into opening a RAR archive and running an executable.
* The group has sent malicious files via email that tricked users into clicking Enable Content to run an embedded macro and to download malicious archives.

Persistence and Privilege Escalation:

* The group saved malicious files within the AppData and Startup folders to maintain persistence
* The group has created scheduled tasks to persistently run VBScripts.

Defense Evasion:

* The group decompresses ZIP files once on the victim machine.
* The group has delivered compressed executables within ZIP files to victims.
* The group has used forged Microsoft code-signing certificates on malware.
* The group has used msiexec.exe to execute an MSI payload.

Credential Access:

* The group used the public tool BrowserPasswordDump10 to dump passwords saved in browsers on victims.

Discovery

* The thread actors obtained a list of active processes on the victim and sent them to C2 servers.

Command and control:

* The group used executables to download malicious files from different sources.