Hive Pro

THREAT ADVISORY

Threat Campaign by Molerats uses NimbleMamba Malware to target Middle East	TA2022032
Threat Level RED	**Publish Date –** Feb 14, 2022

An APT group Molerats associated with Gaza has launched a new threat campaign using a malware NimbleMamba aimed at Middle Eastern governments, foreign policy think tanks, and even a state-owned airline.

The current attack was initiated by spear-phishing emails including links to malware files. Later attacks entice users to download malware file by redirecting them to Dropbox URLs and WordPress sites . Geofencing techniques were employed by the attackers to ensure that only inhabitants of the target nations were directed to the landing page. The final payload was a malicious RAR file containing the NimbleMamba malware and, on occasion, a trojan called 'BrittleBush.'

NimbleMamba has the typical capabilities of an intelligence-gathering trojan, taking screenshots and acquiring process information from the host computer. Additionally, it can detect user interaction, such as looking for mouse movement. The malware also uses the Dropbox API for both C2 as well as exfiltration.

The Techniques commonly used by Molerats are:
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0011: Command and Control
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1059.001: Command and Scripting Interpreter: PowerShell
T1059.005: Command and Scripting Interpreter: Visual Basic
T1059.007: Command and Scripting Interpreter: JavaScript
T1555.003: Credentials from Password Stores: Credentials from Web Browsers
T1140: Deobfuscate/Decode Files or Information
T1105: Ingress Tool Transfer
T1027: Obfuscated Files or Information
T1566.001: Phishing: Spearphishing Attachment
T1566.002: Phishing: Spearphishing Link
T1057: Process Discovery
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.007: Signed Binary Proxy Execution: Msiexec
T1553.002: Subvert Trust Controls: Code Signing
T1204.001: User Execution: Malicious Link
T1204.002: User Execution: Malicious File

Hive Pro

THREAT ADVISORY

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Molerats (Extreme Jackal, Gaza Cybergang, Gaza Hackers Team, TA402, Aluminum Saratoga, ATK 89, TAG-CT5)	Gaza	Afghanistan, Algeria, Canada, China, Chile, Denmark, Egypt, Germany, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Latvia, Libya, Macedonia, Morocco, New Zealand, Oman, Palestine, Qatar, Russia, Saudi Arabia, Serbia, Slovenia, Somalia, South Korea, Syria, Turkey, UAE, UK, USA, Yemen	Aerospace, Defense, Embassies, Energy, Financial, Government, High-Tech, Media, Oil and gas, Telecommunications	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
SHA-256	430c12393a1714e3f5087e1338a3e3846ab62b18d816cc4916749a935f8dab44, c61fcd8bed15414529959e8b5484b2c559ac597143c1775b1cec7d493a40369d, 925aff03ab009c8e7935cfa389fc7a34482184cc310a8d8f88a25d9a89711e86, 2e4671c517040cbd66a1be0f04fb8f2af7064fef2b5ee5e33d1f9d347e4c419f
Domain	uggboots4sale[.]com, easyuploadservice[.]com

References

https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage