MITRE-ID: G0063

Name: BlackOasis

Country: Middle East

Description:

BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. A group known by Microsoft as NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.

TTPs:

1. The exploit was delivered through a Microsoft Office document and the final payload was the latest version of FinSpy malware.
2. This group’s first stage shellcode contains a NOP sled with alternative instructions that was likely designed to bypass antivirus tools.
3. The attack started to deliver Office documents, for example via e-mail. An ActiveX object which contains the Flash exploit was embedded in the document.
4. The Flash object used an ActionScript to extract the exploit, which was seen in other FinSpy exploits.
5. The group contained code to avoid detection by anti-virus software.
6. The first stage shellcode will download 2nd stage codes.
7. The group will inject FinSpy into Winlogon process
8. The group utilized zero days exploits

Reference:

https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/