
BLACK
OASIS
AXIAL

A SURVEY ON BLACK OASIS: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Black Oasis is a Middle-Eastern Threat Group that has been active since 2015 and has been targeting countries like Afghanistan, Angola, Bahrain, Iraq, Iran, Jordan, Libya, The Netherlands, Nigeria, Russia, Saudi Arabia, Tunisia, and the UK with the motivation of Information Theft and Cyberespionage. It is believed that they are a customer of the Gamma Group.

II. TARGET SECTORS

The Group has shown Interest in figures in United Nations as well as opposition bloggers, activists, regional news correspondents, and think tanks.

III. METHODS USED

The Group actively exploited Adobe 0day exploits to deliver malware as well as Phishing and Social Engineering.

IV. ENGAGEMENTS

- In 2015, FinSpy installation packages were delivered through CVE-2015-5119 and CVE-2016-0984 exploitation.
- In 2016, Adobe warned of a vulnerability (CVE-2016-4117) affecting Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. Black Oasis was exploiting this vulnerability.
- In 2017, FireEye had discovered a malicious Microsoft Office RTF document that leveraged CVE-2017-8759. This vulnerability allowed actors to inject arbitrary code to download and execute VB Script that contained PS commands.
- In October 2017, Kaspersky identified a new Adobe Flash 0day exploit being used by Black Oasis. The exploit was delivered through an MS Office document and the final payload was FinSpy Malware.

AX1AL

V. ATTRIBUTIONS

- The use of FinFisher/FinSpy was attributed initially to Black Oasis back in 2016. As such their Operation only exploited Adobe 0days and dropped FinSpy Malware, there isn't much on account of attribution for that.

VII. IOC

C2

1. 89.45.67.107
2. 141.255.166.169

MD5

- 4a49135d2ecc07085a8b7c5925a36c0a
- 8cbaf8c9b4bece4ea0f8cbb80266620e
- a7b990d5f57b244dd17e9a937a41e7f5
- fe5c4d6bb78e170abf5cf3741868ea4c

CVE

1. CVE-2015-5119
2. CVE-2016-0984
3. CVE-2016-4117
4. CVE-2017-8759
5. CVE-2017-11292

VIII. REFERENCES

- https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
- https://apt.securelist.com/apt/blackoasis
- https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html