

Dragon News Blog

January 26, 2022 <https://team-cymru.com/blog/2022/01/26/analysis-of-a-management-ip-address-linked-to-molerats-apt/>

Josh Hopkins < <https://team-cymru.com/blog/author/jhopkinstc/> >

Analysis of a Management IP Address linked to Molerats APT

Enrichment of Zscaler Research into Middle Eastern Espionage Attacks

Key Findings

- Higher order infrastructure, utilizing IP addresses assigned to Palestinian providers, identified for the Molerats APT group
- Additional 'attacker' hosts identified (**23.237.73[.]126** and **45.128.73[.]179**), used to target entities in Israel and Saudi Arabia.

Introduction

On 20 January 2022, Zscaler released a [research blog](#) <

<https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east>> detailing a Molerats espionage campaign against targets in the Middle East, which had commenced in July 2021.

Molerats < <https://attack.mitre.org/groups/G0021/>>, often referred to as the 'Gaza Cybergang', are an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's targets are primarily located in the Middle East, Europe, and the United States.

Zscaler's analysts had identified a screenshot from an attacker machine (see *Figure 1 below*), which they believed had been inadvertently uploaded whilst the actors were testing malware. Within the screenshot an IP address, seemingly used to access the attacker machine, was identified – **185.244.39[.]105**.

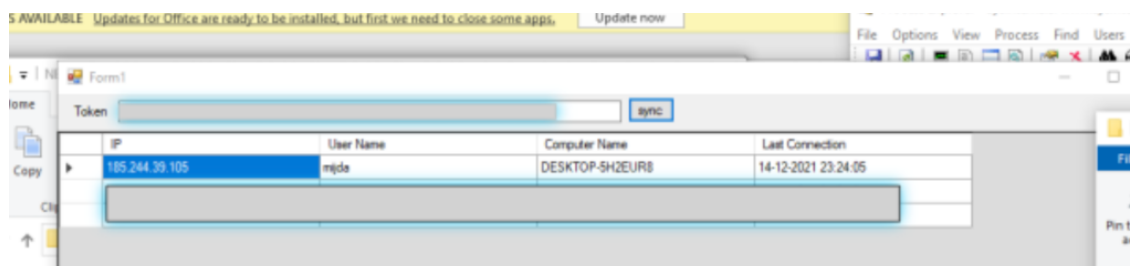


Figure 1: Screenshot of the Attacker Machine (Source – [Zscaler](https://www.zscaler.com/cdn-cgi/image/format=auto/sites/default/files/images/blogs/Molerats%20-%20Dec%202021/Attacker%20Machine%20-%20Snapshot.png) <

<https://www.zscaler.com/cdn-cgi/image/format=auto/sites/default/files/images/blogs/Molerats%20-%20Dec%202021/Attacker%20Machine%20-%20Snapshot.png>>)

In this blog we will explore activity surrounding **185.244.39[.]105** in further detail, using Team Cymru's **Pure Signal™ Recon** < <https://team-cymru.com/products/pure-signal-recon-threat-hunting-and-threat-reconnaissance/>> platform.

Network Telemetry

185.244.39[.]105

When examining network telemetry data for **185.244.39[.]105** over the past few months, inbound connections to TCP/61003 were identified, with directionality inferred based on the ephemeral ports used by the peer IP addresses (see *Figure 2 below for an example of this activity*).

Proto	Client IP Address	Client Port	Server Port	Server IP	Flow Count	Elapsed Time	Start Time	End Time
6 (TCP)	176.106.44.57	62030	61003	185.244.39.105	1111	05:21:46	2021-11-24 06:17:53	2021-11-24 11:39:39
6 (TCP)	185.244.39.105	61003	11712	176.106.47.69	869	05:31:16	2021-11-20 06:26:55	2021-11-20 11:58:11
6 (TCP)	185.244.39.105	61003	57752	45.158.159.37	832	04:34:22	2021-12-19 06:27:57	2021-12-19 11:02:19
6 (TCP)	185.244.39.105	61003	33153	45.158.159.37	828	04:59:23	2021-12-11 08:51:06	2021-12-11 13:50:29
6 (TCP)	185.244.39.105	61003	38826	45.130.98.193	597	03:45:35	2021-10-21 05:18:54	2021-10-21 09:04:29
6 (TCP)	185.244.39.105	61003	28175	176.106.44.129	556	03:40:53	2021-12-28 06:20:59	2021-12-28 10:01:52
6 (TCP)	176.106.44.57	61884	61003	185.244.39.105	514	02:31:55	2021-11-25 08:29:47	2021-11-25 11:01:42

Figure 2: Activity on 185.244.39[.]105:61003

In total, connections were observed from ten distinct IP addresses (see *Table 1 below*) assigned to SPEED-CLICK-LIMITED, PS, with traffic most recently observed on 06 January 2022. Geolocation data placed a number of these IP addresses in the Gaza Strip.

IP Address	First Seen	Last Seen
45.130.98[.]193	2021/10/21 05:18:54	2021/10/26 06:59:20
45.130.98[.]194	2021/10/26 07:05:48	2021/11/02 11:49:02
176.106.47[.]69	2021/11/20 06:26:55	2021/11/21 08:25:42
176.106.44[.]164	2021/11/21 08:28:46	2021/11/21 09:04:04
176.106.44[.]57	2021/11/21 09:12:18	2021/11/25 11:35:11
45.158.159[.]37	2021/12/05 07:53:38	2021/12/19 12:14:26
176.106.47[.]3	2021/12/20 07:29:07	2021/12/21 12:27:43
176.106.47[.]141	2021/12/22 06:34:14	2021/12/27 12:47:27
176.106.44[.]129	2021/12/28 06:20:59	2021/12/30 11:52:51

176.106.45[.]99	2022/01/02 07:09:28	2022/01/06 11:40:23
-----------------	---------------------	---------------------

Table 1: IPs Connecting to 185.244.39[.]105:61003

As can be seen in Table 1, the relationship between the listed IPs and **185.244.39[.]105** is sequential, with no cross-over in use observed in the first and last seen timestamps.

This activity is indicative of one user/machine being utilized to access 185.244.39[.]105 over an extended time period, with the client IP address refreshing due to DHCP lease renewal; SPEED-CLICK-LIMITED is a home broadband provider (wireless and ADSL).

Given this pattern of IPs assigned to the same provider (SPEED-CLICK-LIMITED, PS) being utilized to connect to an IP associated with the Molerats APT group, we decided to examine network telemetry data, during the time periods specified, for each of the IPs listed in Table 1.

23.237.73[.]126

In each case, outbound sessions to remote UDP/46370 on **23.237.73[.]126** were observed (see *Figure 3 below for an example of this activity*). This IP address is assigned to FDCSERVERS, US – an American hosting/VPS provider.















Proto	Client IP Address	Client Port	Server Port	Server IP	Flow Count	Elapsed Time	Start Time	End Time
17 (UDP)	23.237.73.126 	46370	30051	45.130.98.193 	1376	06:22:06	2021-10-25 04:55:01	2021-10-25 11:17:07
17 (UDP)	45.158.159.37 	52968	46370	23.237.73.126 	1374	05:17:37	2021-12-19 06:36:28	2021-12-19 11:54:05
17 (UDP)	23.237.73.126 	46370	15905	45.130.98.194 	1252	05:40:23	2021-10-31 06:31:14	2021-10-31 12:11:37
17 (UDP)	23.237.73.126 	46370	15909	176.106.47.69 	1179	05:46:20	2021-11-20 06:33:40	2021-11-20 12:20:00
17 (UDP)	176.106.44.57 	61568	46370	23.237.73.126 	943	05:02:45	2021-11-22 06:14:28	2021-11-22 11:17:13
17 (UDP)	176.106.44.57 	51215	46370	23.237.73.126 	858	05:41:53	2021-11-24 05:53:44	2021-11-24 11:35:37
17 (UDP)	45.130.98.193 	58366	46370	23.237.73.126 	828	05:47:12	2021-10-24 05:26:16	2021-10-24 11:13:28

Figure 3: Activity on 23.237.73[.]126:46370

Network telemetry data for **23.237.73[.]126** identified connections to remote

TCP/443 on an IP address assigned to a provider in Saudi Arabia (see Figure 4 below). This activity occurred between 21 – 22 December 2021. Passive DNS data for this IP address identified it as a mail server for the Secretariat General of a regional government organization in the Middle East.

Start Time	Src IP	Dest IP	Proto	Src Port	Dest Port	TCP Flags	Packets	Bytes
2021-12-21 07:37:17	23.237.73.126	[REDACTED]	6 (TCP)	60742	443 (https)	16 (ACK)	3000	156000
2021-12-21 07:51:01	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	192000
2021-12-21 07:52:55	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	156000
2021-12-21 08:00:20	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	156000
2021-12-21 08:03:34	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	156000
2021-12-21 08:05:28	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	156000
2021-12-21 08:05:46	23.237.73.126	[REDACTED]	6 (TCP)	33872	443 (https)	16 (ACK)	3000	156000

Figure 4: Outbound Activity from 23.237.73.[.]126

When reviewing inbound network telemetry data for **23.237.73.[.]126:46370**, a further three IP addresses were observed in UDP sessions:

- **85.114.96.[.]246**
- **85.114.102.[.]90**
- **85.114.112.[.]152**

All three IP addresses were assigned to FUSION-SERVICES, PS, with geolocation data again placing them in the Gaza Strip.

As previously, a pivot was undertaken on these IP addresses in order to identify further Molerats APT infrastructure.

45.128.73.[.]179

Two of the IP addresses assigned to FUSION-SERVICES, PS were observed in outbound sessions to remote UDP/47489 on **45.128.73.[.]179**. This IP address is assigned to DEDIPATH, US – an American hosting/VPS provider.

In addition, five of the IP addresses contained in Table 1, as well as a further IP address (**45.130.98.[.]149**) assigned to SPEED-CLICK-LIMITED, were observed in UDP sessions to **45.128.73.[.]179:47489**

can be seen to reflect a similar pattern.

Furthermore, inbound connections to TCP/61637 on **45.128.73[.]179** were observed from three of the IP addresses accessing **45.128.73[.]179:47489**.

Proto	Client IP Address	Client Port	Server Port	Server IP	Flow Count	Elapsed Time	Start Time	End Time
17	45.128.73.179	47489	22417	45.158.159.37	126	03:37:23	2021-12-14 08:43:07	2021-12-14 12:20:30
17	45.128.73.179	47489	39681	45.130.98.194	103	00:37:37	2021-11-10 10:29:01	2021-11-10 11:06:38
17	45.128.73.179	47489	35501	176.106.44.57	85	00:57:21	2021-11-25 07:14:10	2021-11-25 08:11:31
17	45.128.73.179	47489	43952	85.114.112.152	78	04:28:59	2021-11-20 07:20:33	2021-11-20 11:49:32
17	45.128.73.179	47489	27372	176.106.47.3	59	00:42:11	2021-12-21 08:17:54	2021-12-21 09:00:05
6	45.128.73.179	61637	15749	45.130.98.149	58	00:33:10	2021-11-30 11:51:09	2021-11-30 12:24:19
17	45.128.73.179	47489	47772	176.106.47.3	58	00:19:48	2021-12-20 06:36:57	2021-12-20 06:56:45

Figure 5: Inbound Activity for 45.128.73[.]179

Network telemetry data for **45.128.73[.]179** identified connections to remote TCP/443 on an IP address assigned to an Israeli provider. This activity occurred on 15 January 2022. Passive DNS data for this IP address identified it as a web server for an Israeli government department.

Summary

Figure 6 (below) provides a summary of all the network telemetry data discussed so far in this blog, showing the links between the higher order infrastructure and ‘attacker’ hosts.

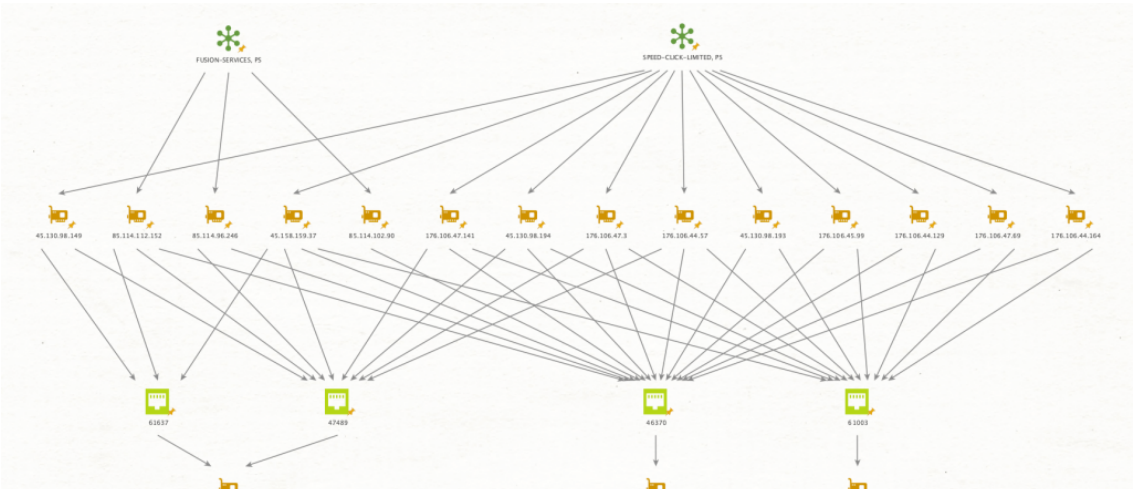




Figure 6: Molerats APT Infrastructure

Commonalities

Open ports information for the three IP addresses identified at the bottom of Figure 6 as attacker infrastructure, showed that each host was running an Apache web server on TCP/80; version 2.4.18 (Ubuntu). Open source information indicated that in each case, this Apache version was first observed around June / July 2021. A variety of CVEs are reported for Apache version 2.4.18, dating back to 2016. It is possible that Molerats APT actors compromised these hosts for use in attack activity, although an alternative theory might be that the actors are using an outdated version of Apache in the setup of their C2 servers.

Given the apparent vulnerability of these servers, it should be noted that other malicious actors may have gained access during the period of activity examined in this blog.

Conclusion

From the starting point of an IP address (**185.244.39.[.]105**) associated with the management of an 'attacker machine', it was possible to pivot and identify higher order infrastructure utilizing IP addresses assigned to a Palestine provider. From this point a further pivot led us to the identification of an additional 'attacker' host (**23.237.73.[.]126**), based on observed connections to the mail server of a Middle Eastern government organization during December 2021.

Although it was possible to confirm successful connections were made to the mail server (based on observed TCP flags), it is unclear whether the Molerats APT actors were able to gain access to specific mailboxes (although this was the

hypothesized intent).

Travelling back upstream from this new 'attacker' host, it was possible to identify further higher order infrastructure, which led to another 'attacker' host (45.128.73[.]179) being identified. In this case based on connections to an Israeli government web server during January 2022.

Based on these observations, it is apparent that the infrastructure first identified by Zscaler and expanded upon in this blog, is being utilized in current and ongoing operations attributable to the Molerats APT group.

Indicators of Compromise

23.237.73[.]126

45.128.73[.]179

← [The Biggest Cyber Security Developments in 2021](https://team-security-developments.cymru.com/blog/2021/12/21/the-biggest-cyber-security-developments-in-2021/) < [https://team-security-developments-in-2021/>](https://team-security-developments.cymru.com/blog/2021/12/21/the-biggest-cyber-security-developments-in-2021/)

Subscribe Now

