# Alien Labs 2019 Analysis of Threat Groups Molerats and APT-C-37

cybersecurity.att.com/blogs/labs-research/alien-labs-2019-analysis-of-threat-groups-molerats-and-apt-c-37

1. AT&T Cybersecurity
2. Blog

January 15, 2020 | Fernando Martinez

In 2019, several industry analyst reports confused the threat groups Molerats and APT-C-37 due to their similarity, and this has led to some confusion and inaccuracy of attribution.

For example, both groups target the Middle East and North Africa region (with a special emphasis on Palestine territories). And, they both approach victims through the use of phishing emails that contain decoy documents (mostly in Arabic) and contain themes concerning the political situation in the area.

To improve understanding of the differences and similarities of the two groups (as well as the links between them), we at Alien Labs™ are providing an analysis of their 2019 activity.


A recent spear-phishing document from Molerats

## APT-C-37 Overview

**APT-C-37**, also known as Pat-Bear or the Syrian Electronic Army (SEA), was first seen in October 2015 targeting members of a terrorist organization. Since 2015, however, APT-C-37 has broadened their objectives to include government agencies, armed forces leadership, media organizations, political activists, and diplomats. The group mostly targets victims in Western countries, with the intent of defacing their websites and social accounts while leaving a public footprint after hacking one of their victims.

In previous attacks, APT-C-37 targeted Windows and Android systems, utilizing popular commercial remote access trojans (RATs) such as DroidJack, SpyNote, njRAT, SSLove, and H-Worm.

### Technical Analysis: APT-C-37 2019

**June 2019: APT-C-37 released an Android app named after the instant messaging software "WhatsApp" as an espionage tool to reportedly spy on the Syrian opposition forces. The app was capable of installing the SSLove RAT to pull private information from the phone and exfiltrating it to a remote location.**

## Molerats Overview

Molerats has been present in the cybercriminal landscape since 2012. In an analysis released by the Kaspersky's GReAT (Global Research & Analysis Team) earlier this year on the Gaza Hacker Team and their various subgroups, Kaspersky concluded that Molerats is Gaza Cybergang "Group1." The report also concluded that Molerats (i.e. Cybergang Group 1) operates with a lower level of sophistication than other groups within the Gaza Hacker Team. In addition, a 2016 article in Security Week reported that one of Molerats campaigns (October 2016) heavily used popular RATs like NjRat and H-Worm (aka Houdini).

## Technical Analysis: Molerats 2019

**October 2019**: In Molerats' October operation, the attack was distributed as a phishing campaign in the Middle East. Emails included a Microsoft Word file attachment with the title "Daily report on the most important Palestinian developments for the day 9-9-2019.doc" — content that spoke to the political situation in Palestine. When a victim opened the attachment, the malware performed the following:

- Displayed the Microsoft Word document as distraction.
- Unpacked a Microsoft.vbs into the folder 'C:\programdata\Micorsoft' to confuse the victim with a typo inside the folder 'Micorsoft'.
- Programmed itself as a scheduled task, once the previous vbs was executed.
- Made an HTTPS request to download GoogleChrome.vbs, which had an additional HTTPS request to GoogleChrome.msi. (This file, an additional MSI file and potentially the RAT to infect the system, was not available at the time of the investigation.)

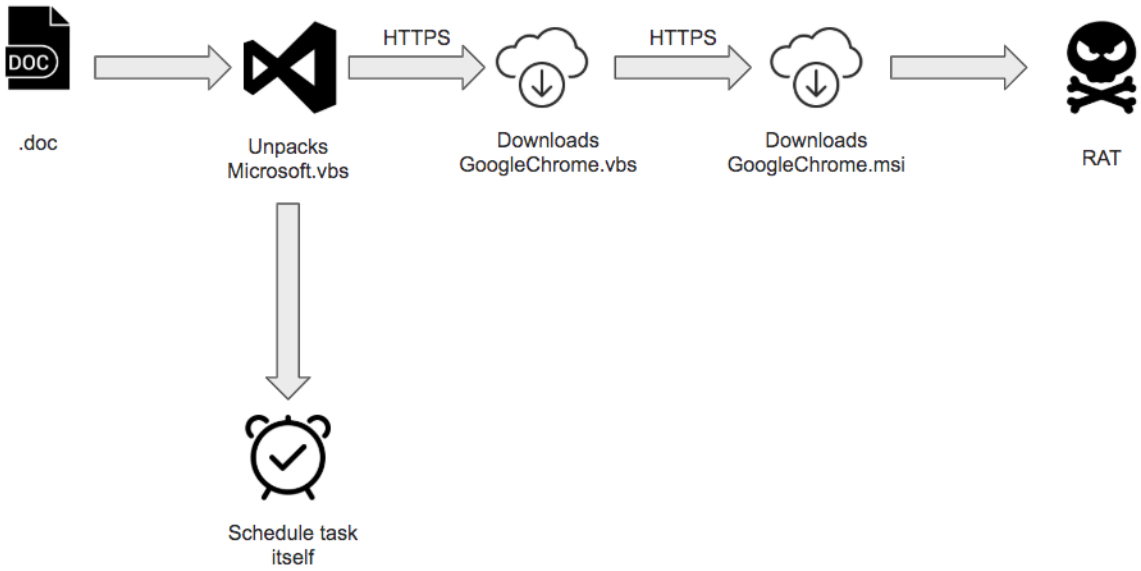


Diagram of Molerats October 2019 campaign

**September-October 2019**: In Molerat's September campaign, the malware propagated through an executable with a fake PDF file. With the names "The case of Muath Ismail Haniyeh.pdf.exe" and "Interface.pdf.exe," the executables are both signed under the name "FoxitReader."

When a victim opened the attachment, the malware performed the following:

- Both documents extracted an executable and then a PDF to distract the user.
- The executable with names FoxitReader.exe or NEG.exe contained a copy of the Perseus Trojan (despite both being signed by FoxitReader), which communicated with the command and control (C&C) infrastructure through HTTPS.

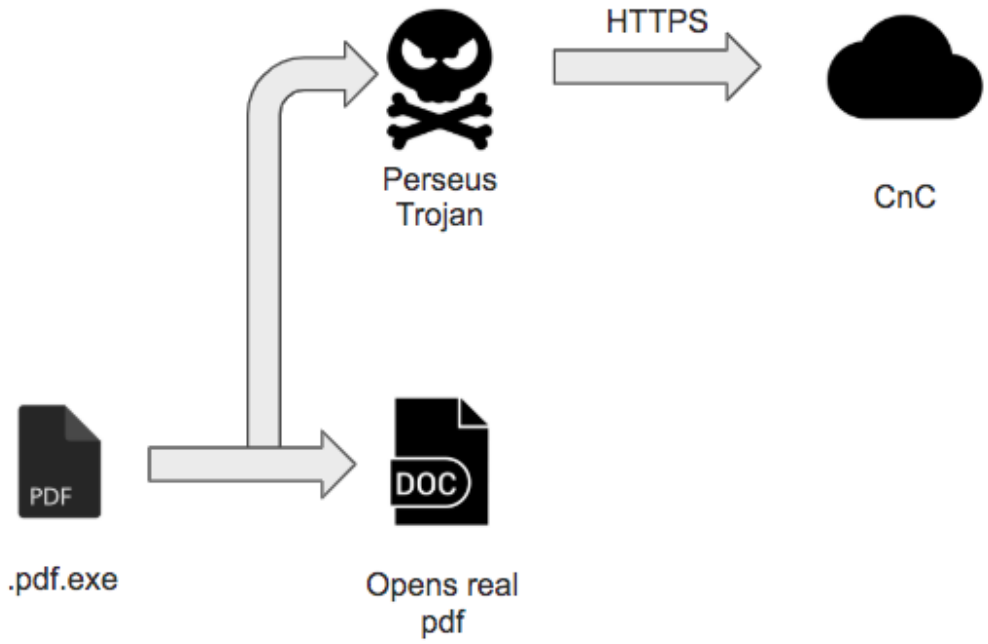


Diagram of Molerats September – October 2019 campaign

**August 2019**: In August, Molerats ran another campaign, however we did not detect the use of phishing. Instead, Alien Labs identified a sample communicating with a new domain that used the same C&C pattern detected by an IDS signature. You can find details and more on the Open Threat Exchange (OTX). The domain, which has been up since 2017, has two malicious files associated with it:

- The first file matched the same IDS signature. See additional info at OTX.

- The second file was first uploaded to VirusTotal back in 2018, but Alien Labs recently rescanned the file and found the latest domain (www.freshchrysanthemum[.]com). At the time of the analysis, the C&C was down or filtering the connection. Some of the other public sandboxes such Hybrid Analysis and JoeSandbox exhibit the same behavior. An analysis of the sample by Any.run was able to resolve the domain and reach to it with an IP in Norway (82.102.22.109). See additional info at OTX.

**January 2019:** In January, Molerats switched its tactics back to phishing with Word Documents that concealed a malicious Vbscript. The vbs contained an encoded version of the malware, which was scheduled and executed after decryption. The malicious file corresponded to a version of the Fraudrop Trojan, packed with Enigma as previously seen in other Molerats' samples, and it used the Simple and Fast Multimedia Library (SMFL), which is commonly used for game development.

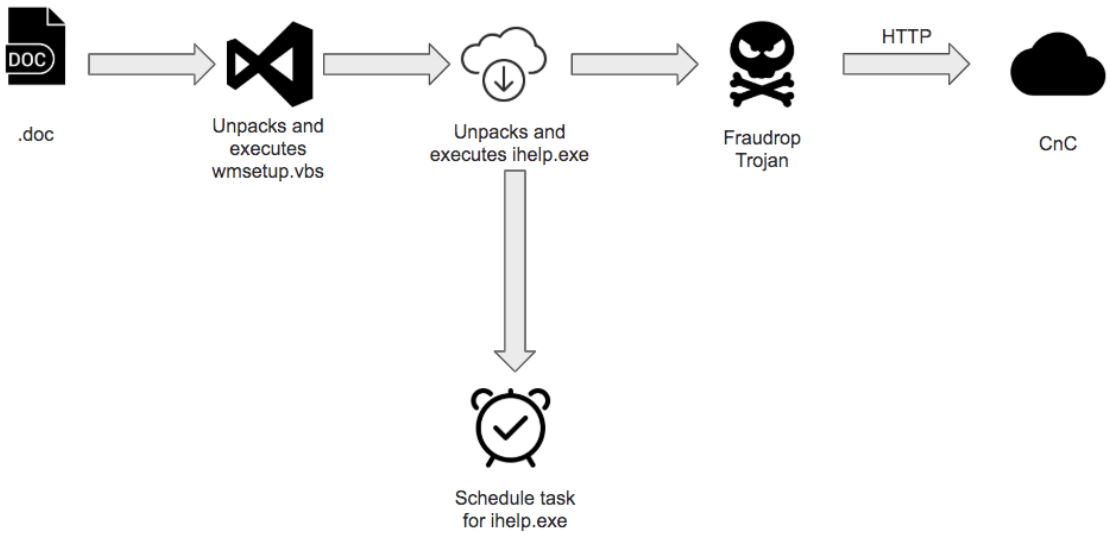


Diagram of Molerats January 2019 campaign

**November 2019**: In November, Alien Labs discovered a new Molerats sample. In this case, the group recycled the domain used in their January attack for C&C. In this campaign, an executable with an Arabic name that translates to "Winter government by names," extracted and executed a modified version of the Fraudrop trojan. Molerats had attempted to hide the packer they were using and they modified the filename, however the C&C and Beacon they used were the same and they were using the SMF library for development.

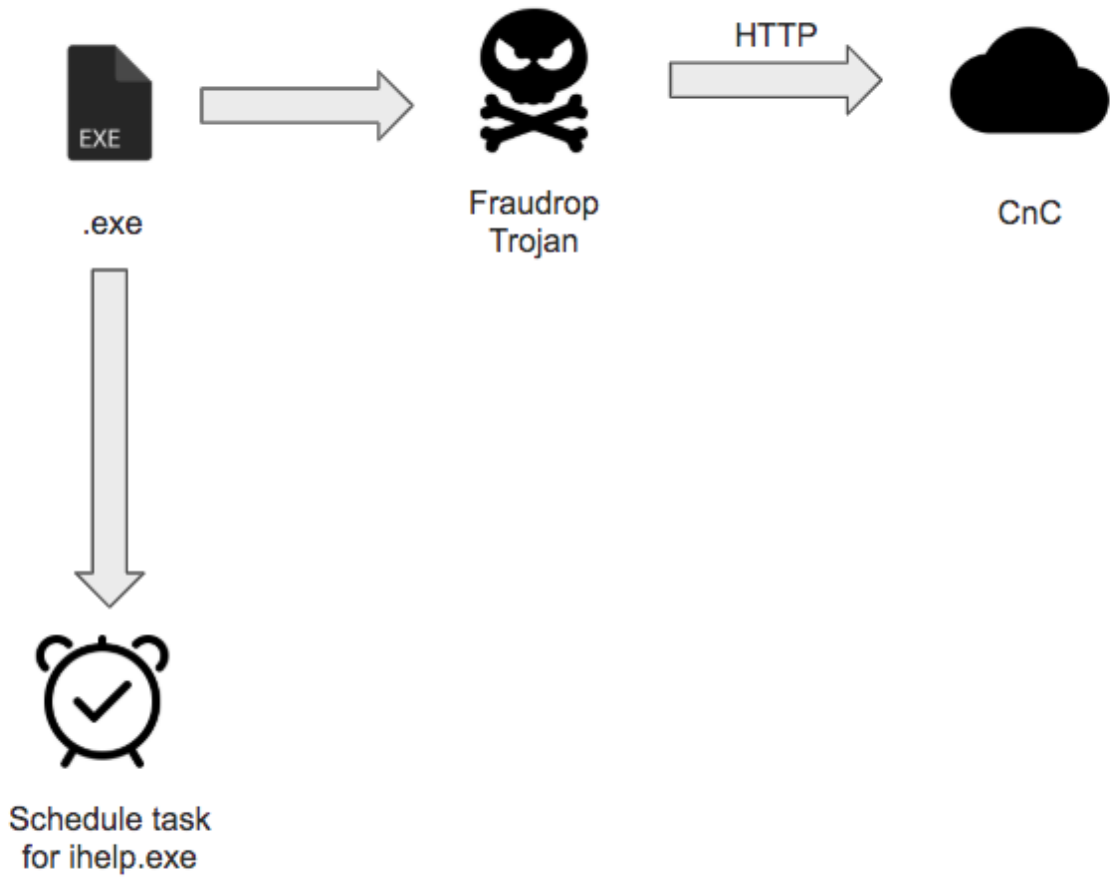


Diagram of Molerats November 2019 campaign

## APT-C-37 vs. Molerats

| | APT-C-37 | Molerats |
|---|---|---|
| **Names** | • Pat-Bear<br>• Syrian Electronic Army | • Gaza Cybergang<br>• Gaza Hacker Team<br>• Molerats (Gaza Cybergang Group1)<br>• Desert Falcons (Gaza Cybergang Group2)<br>• Operation Parliament (Gaza Cybergang Group3)<br>• SneakyPastes (Campaign by Molerats)<br>• DustySky<br>• Moonlight |

| | | |
|---|---|---|
| **Targets** | • Armed organizations<br>• Israel<br>• Egypt<br>• Occidental countries | Middle East North Africa region, especially Palestinian territories |
| **Timelines** | Since October 2015 (as the Syrian Electronic Army, since 2011) | Since 2012 |
| **Tactics** | RATs like DroidJack, SpyNote, njRAT, or H-Worm.<br><br>Windows and Android attacks.<br><br>Tends to leave public signatures for everyone to show they hacked their victims or leak exfiltrated data. | Phishing campaigns with MS Word documents or PDF files with the malware packed inside the document or retrieved through HTTPS.<br><br>Persistence is obtained through scheduled tasks.<br><br>Malware is not a constant and malware is heavily rotated, but C&C are sometimes recycled. |

## Is this a Molerats or APT-C-37 attack?

The three attacks below have been attributed to APT-C-37 and Molerats, however it's our opinion at Alien Labs that they don't share the clear patterns of Molerats or APT-C-37 we've seen prior to this blog.

**November 2019 (Palestinian election): Attributed on Twitter by Rising Enterprise Security to APT-C-37**

This campaign tried to utilize the Palestinian elections as a theme for their phishing emails, and the target appeared to be the Palestinian government. We observed the use of phishing emails in the campaign with fake documents themed after the elections that contained at least two different malicious files. The file names are (translated here):

- Election Committee Meeting - Northern Territory.exe
- Majdalani seriously doubts President Abbas about the presidential election.exe

Both files used a Microsoft Word icon in attempt to make the victims run the malicious executable. When executed it performed the following.

- Extracted and opened a relevant Word document into the temp folder to lure the target.

- Extracted a LNK file (a file extension for a shortcut **file** used by Microsoft Windows to point to an executable file**)** and used it to achieve persistence in the system. The LNK file was camouflaged under the name “HelpPane.lnk,” so it could execute the next step of future campaigns.
- Downloaded a script that included mshta.exe (a utility that executes Microsoft HTML Applications), which then downloaded an additional script that included a PowerShell.
- Finally, downloaded and executed a RAT, in particular the popular Houdini RAT (also known as H-worm).

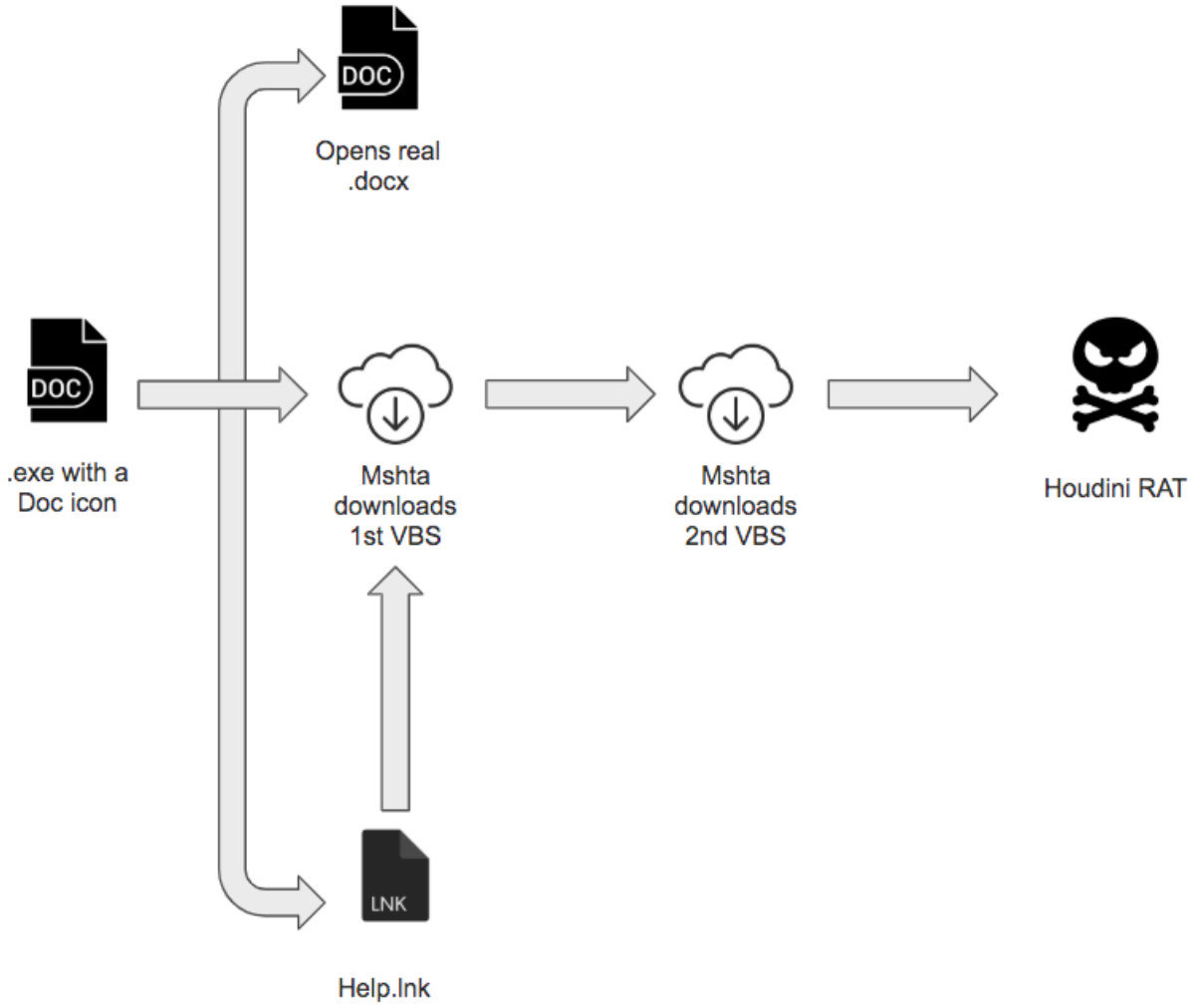


Diagram of November 2019 attributed on Twitter to APT-C-37

**August 2019**: **Attributed on Twitter to APT-C-37**

This attack, attributed to APT-C-37 on Twitter, is very similar to the November 2019 attack described above, however it did not use the Palestinian elections to lure victims. This time, the threat group used another .exe which included a decoy Word document titled “A new

scandal for a Hamas leade*r”*. The execution was very similar to the November 2019 campaign, however this time the camouflaged LNK file was “History.lnk” and it installed a version of Houdini RAT.

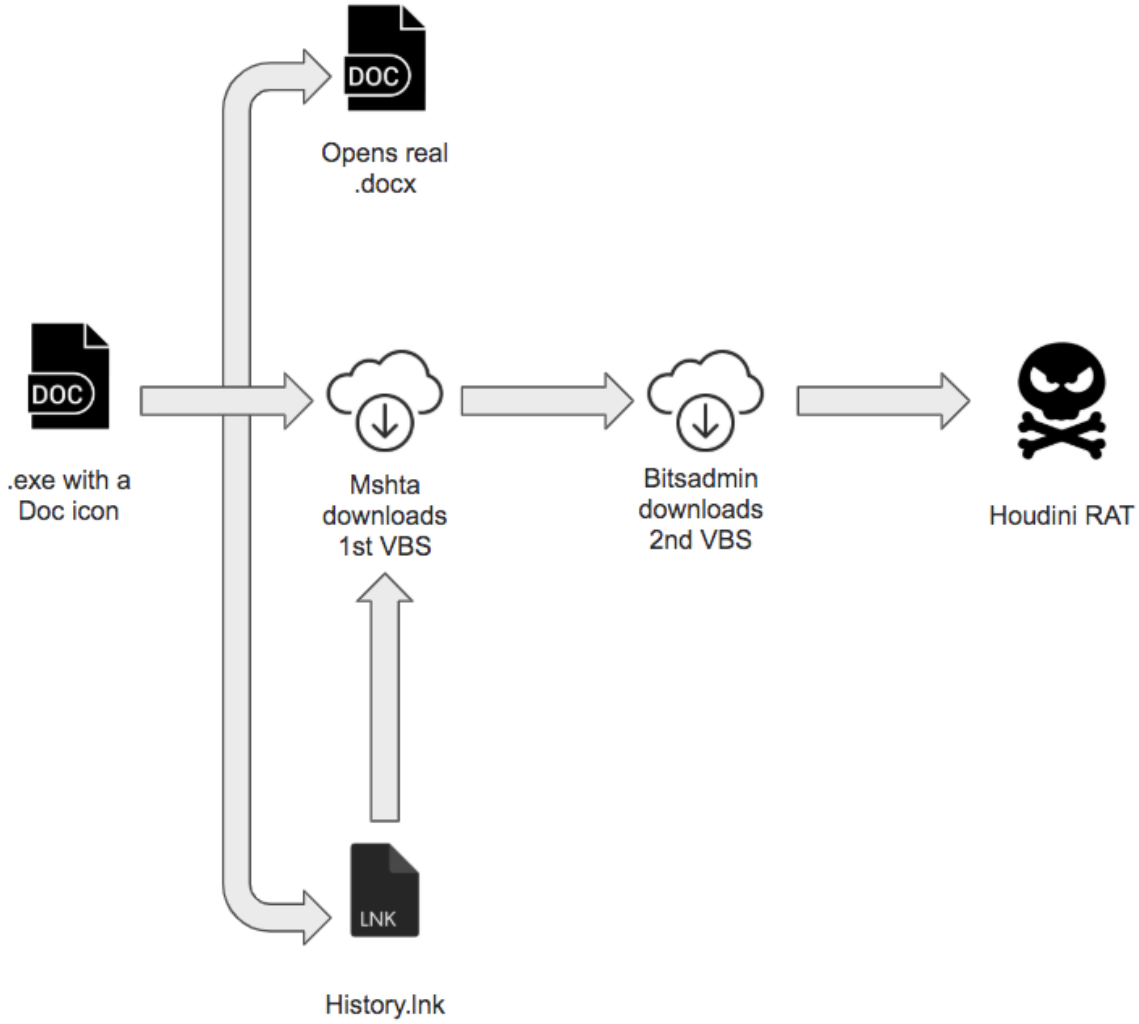


Diagram of August 2019 campaign attributed on Twitter to APT-C-37

**April 2019**: **Attributed on Twitter to APT-C-37**

In April 2019, security researchers on Twitter observed another phishing email with an attached executable. When executed, the malware opened a document talking about the Palestinian Ministers to keep the victim entertained while it installed a LNK file “MsOfficee.lnk,” which is very close to the real “MsOffice.lnk.” The file allowed the Houdini RAT to execute and gain persistence on the targeted machine.

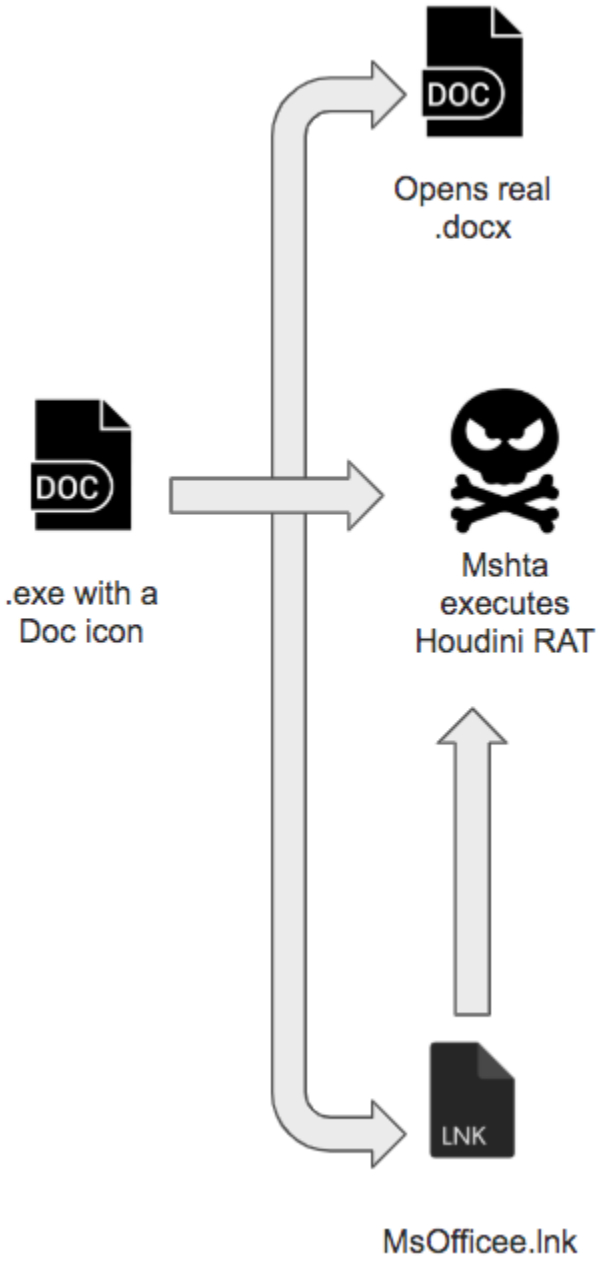


Diagram of **April 2019 campaign attributed on Twitter to APT-C-37**

The three attacks above have the following similar characteristics:

- They used phishing documents themed on Palestine.
- .exe files opened relevant documents in Arabic.
- The first step executed mshta.exe.
- They obtained persistence in the victim's systems through LNK files with decoy names.
- They used Timeout.exe to pause execution for different times before executing the RAT.
- C&C communication went through HTTP.
- They executed the Houdini RAT.

The above-mentioned target and the delivery methods suggest these attacks are being launched by Molerats (note: the Houdini RAT is very popular in the Middle East and cannot be used for attribution). However, in the opinion of Alien Labs, the other attack patterns make it hard for us to tie these attacks to Molerats or APT-C-37, as they do not have a clear pattern that aligns to the samples previously associated with Molerats or APT-C-37. In light of this, Alien Labs currently buckets these three attacks under an unattributed classification.

## Conclusion

Yes, indeed, we have seen similar patterns between Molerats and APT-C-37 in 2019. However, Molerats has shown to be a more active group (even beyond 2019), with a more advanced tradecraft and methods that are more difficult to defend against due to the use of HTTPS, high rotation of malware, or even IP filtering to specific geolocations. Therefore, we do not have a high level of confidence that the latest samples belong to any of these two groups or have a relationship at this time. Having said this, we offer a caveat: of the samples we analyzed, we left three unattributed for the moment. Through future analysis, we may find that these do fall under either Molerats or APT-C-37. If that happens, we'll keep you updated in OTX.

### Share this with others

Tags: malware, malware research, alien labs, molerats, apt-c-37