

# Operation Parliament, who is doing what?

By [GReAT](#) on April 12, 2018. 7:00 am

## Summary

Kaspersky Lab has been tracking a series of attacks utilizing unknown malware since early 2017. The attacks appear to be geopolitically motivated and target high profile organizations. The objective of the attacks is clearly espionage – they involve gaining access to top legislative, executive and judicial bodies around the world.

1. The attackers have targeted a large number of organizations globally since early 2017, with the main focus on the Middle East and North Africa (MENA), especially Palestine. High-profile organizations have also been targeted in other regions. The number of attacks has decreased since the beginning of 2018.
2. The attacks were initially discovered while investigating a phishing attack that targeted political figures in the MENA region. At first the attacks looked to be the work of the low-sophistication [Gaza Cybergang](#) (decoys, file names), but further analysis painted a very different picture.
3. Targets include high-profile entities such as parliaments, senates, top state offices and officials, political science scholars, military and intelligence agencies, ministries, media outlets, research centers, election commissions, Olympic organizations, large trading companies, and other unknown entities.
4. The malware basically provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute any scripts/commands and receive the result via HTTP requests.
5. Kaspersky Lab users and [Threat Management and Defense](#) clients are protected from the attacks.

[Kaspersky Security Bulletin: Review of the Year 2017](#)

[Kaspersky Security Bulletin: Threat Predictions for 2018](#)

[Threat Predictions for Industrial Security in 2018](#)

[Kaspersky Security Bulletin 2016. Review of the year. Overall statistics for 2016](#)

[Kaspersky Security Bulletin. Predictions for 2017](#)

[Kaspersky Security Bulletin 2015. Evolution of cyber threats in the corporate sector](#)



**KASPERSKY LAB:  
PLATINUM AWARD**

Gartner Peer Insights Customer Choice Award for Endpoint Protection Platforms

[Find out more >](#)

Cisco Talos recently [published a blogpost](#) describing targeted attacks in the Middle East region which we believe may be connected.

## Victimology and Statistics

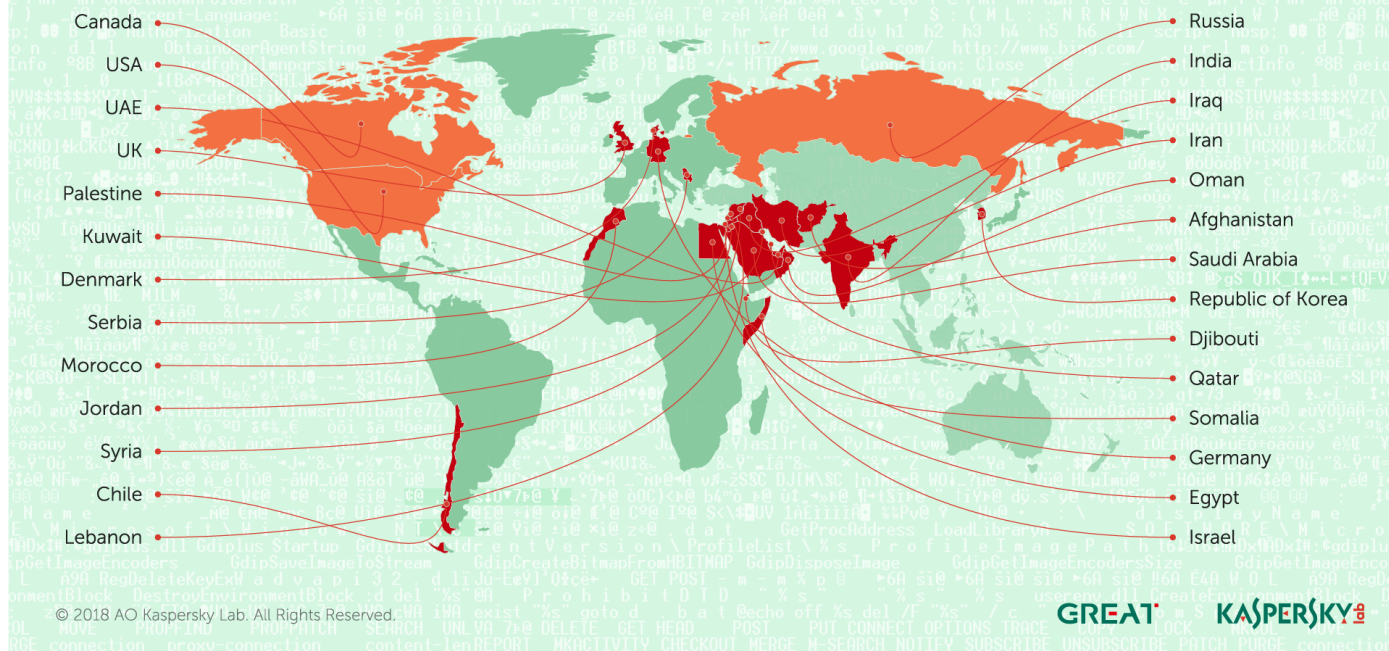
Based on our findings, we believe the attackers represent a previously unknown geopolitically motivated threat actor. The campaign started in 2017, with the attackers doing just enough to achieve their goals. They most likely have access to additional tools when needed and appear to have access to an elaborate database of contacts in sensitive organizations and personnel worldwide, especially of vulnerable and non-trained staff. The victim systems range from personal desktop or laptop systems to large servers with domain controller roles or similar. The nature of the targeted ministries varied, including those responsible for telecommunications, health, energy, justice, finance and so on.

Victims have been spotted in the Palestinian Territories, Egypt, Jordan, the UAE, Saudi Arabia, Djibouti, Qatar, Lebanon, Chile, Somalia, Iraq, Morocco, Syria, India, Iran, Canada, the USA, the UK, Germany, Israel, Afghanistan, Serbia, Russia, Oman, Kuwait, South Korea and Denmark.

<b>Victim organization type</b>	<b>Number of victim organizations</b>
Unknown	91
Senates/Parliaments	7
Prime Ministerial Offices	3
Military/Intelligence Agencies	5
Other Gov./Ministerial/Diplomatic Offices	20
Financial/Banking Institutions	5
Media Outlets	2
Olympic/Sports Bodies	2
Research Centers/Scholars	2
Election Commissions	1

# Operation parliament

New cyberespionage group "Operation Parliament" is targeting high profile organizations from around the world with a focus on the Middle East and North Africa.



The number of victims/victim organizations probably doesn't represent the full scope of the attacks – only a portion.

## Attack description and attribution

Operation Parliament appears to be another symptom of escalating tensions in the Middle East region. The attackers have taken great care to stay under the radar, imitating another attack group in the region. They have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their command and control servers. The targeting seems to have slowed down since the beginning of 2018, probably winding down when the desired data or access was

obtained. The targeting of specific victims is unlike previously seen behavior in regional campaigns by Gaza Cybergang or [Desert Falcons](#) and points to an elaborate information-gathering exercise that was carried out before the attacks (physical and/or digital).

With deception and false flags increasingly being employed by threat actors, attribution is a hard and complicated task that requires solid evidence, especially in complex regions such as the Middle East.

See the following for more information and examples of false flags being used in cyberattacks:

[Wave your false flags! ...or the Nightmares and Nuances of a Self-Aware Attribution Space](#)

[OlympicDestroyer is here to trick the industry](#)

## Malware description

The malware was first seen packed with VMProtect; when unpacked the sample didn't show any similarities with previously known malware. All the strings and settings were encrypted and obfuscated. Functionality was identified that enables HTTP communication with the C&C server and invokes "processcreate" based on parameters received as a response.

The configuration and strings are encrypted using 3DES and Base64 encoding. Data sent to the C&C server is also encrypted using 3DES and Base64. Different keys are used for local and network encryption.

The malware starts communicating with the C&C server by sending basic information about the infected machine. The C&C server then replies with the encrypted serialized configuration.

The malware basically provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute scripts/commands and receive the results via HTTP requests.

```

{"Kaliyah":60,"Kamron":[{"Alaya":662009,
  "Immanuel":"cx30FE4LA4jjMMoXoefx1A==",
  "Olive":true,"Graeme":false,
  "Jadiel":false,
  "Jovani":"z1lxJXy4S1bW5TvgX9NBDeq3WPiU8LjW"}],
{
"Alaya":662010,"Immanuel":"cx30FE4LA4jjMMoXoefx1A==", "Olive":true,"Graeme":false,
"Alaya":662011,"Immanuel":"cx30FE4LA4jjMMoXoefx1A==", "Olive":true,"Graeme":false,
"Alaya":662012,"Immanuel":"cx30FE4LA4jjMMoXoefx1A==", "Olive":true,"Graeme":false,
"Alaya":662013,"Immanuel":"cx30FE4LA4jjMMoXoefx1A==", "Olive":true,"Graeme":false,

```

Sample of the C&C response with encrypted commands and configurations

## Examples of attack decoys



Translation: Contacts list of media personnel



*Translation: Relations between UAE and Jordan, and the impact caused by the non-boycott of Qatar*



Microsoft Word interface showing a document titled "كشف التقاعد 2017 يونيو". The document contains a table with names and titles, partially obscured by a black redaction box.

الاسم	اللقب	الرتبة
احمد	تقريب	رتك
خالد	رتك	رتك
عبدالله	رتك	رتك
عبدالله	ملازم أول	رتك
محمد	رتك	رتك
ماجد	مقدم	رتك
اكرم	رتك	رتك
حسن	رتك	رتك
عائش	مساعد	رتك
ايهاب	مقدم	رتك

Translation: Military retirement statement 2017 June

FILE HOME CREATE EXTERNAL DATA DATABASE TOOLS

View Paste Copy Cut Format Painter Filter Filter Ascending Descending Selection Advanced Remove Sort Toggle Filter Refresh All Save Delete More Find Replace Go To Select B I U A Text Formatting

SECURITY WARNING Some active content has been disabled. Click for more details. Enable Content

2017 حماس

## هيكلية حماس الجديدة لقطاع غزة 2017

اضغط تمكين المحتوى لعرض البيانات

الصورة :

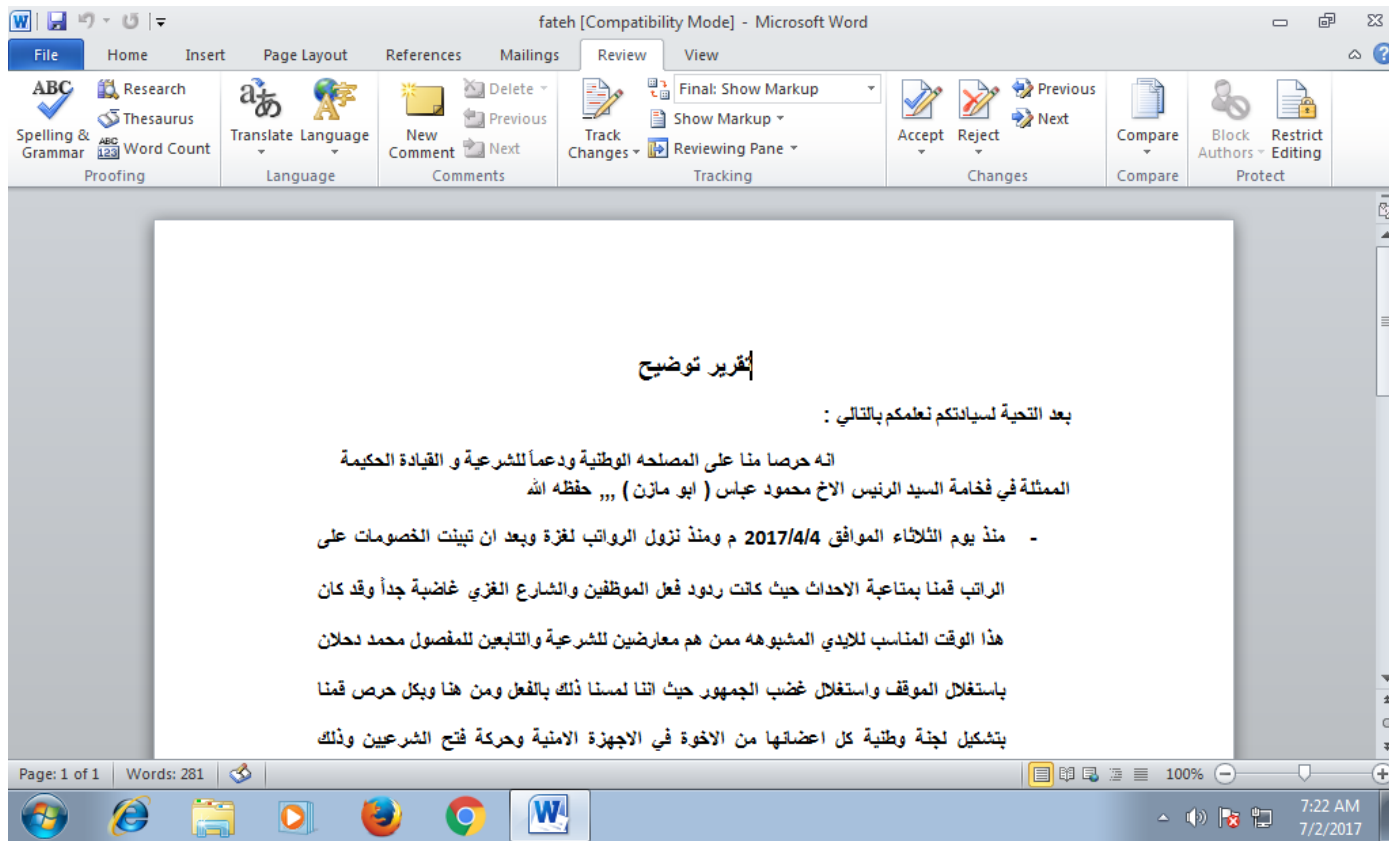


تم تمكين المحتوى لعرض البيانات

الاسم :	تم تمكين المحتوى لعرض البيانات
الحقيبة :	تم تمكين المحتوى لعرض البيانات
العمل الحالي :	تم تمكين المحتوى لعرض البيانات
العمل السابق :	تم تمكين المحتوى لعرض البيانات
المؤهل العلمي :	تم تمكين المحتوى لعرض البيانات
المنطقة :	تم تمكين المحتوى لعرض البيانات
المربع :	تم تمكين المحتوى لعرض البيانات
الرتبة الحركية :	تم تمكين المحتوى لعرض البيانات
الحالة الإجتماعية :	تم تمكين المحتوى لعرض البيانات
المسجد :	تم تمكين المحتوى لعرض البيانات
الراتب :	تم تمكين المحتوى لعرض البيانات

Translation: The new Hamas structure for Gaza strip 2017





*Translation: Clarification report (on Gaza employee salaries)*

## What should high-profile organizations do?

High-profile organizations should have elevated levels of cybersecurity. Attacks against them are inevitable and are unlikely to ever cease. These organizations need to pay particular attention to their security, implementing additional measures to ensure they are well protected. Anti-targeted attack solutions, threat intelligence capabilities and data flows, default-deny application lockdown, endpoint detection and response, data leak and insider threat prevention, and even isolated/air-gapped networks should form the basis of any strategy for protecting organizations in the current threat landscape.

The victims of Operation Parliament need to re-evaluate their approach to cybersecurity.

## Additional information

For more information about the attacks and the indicators of compromise, please contact:

[intelreports@kaspersky.com](mailto:intelreports@kaspersky.com)

Alternatively, please visit: <https://www.kaspersky.com/enterprise-security/apt-intelligence-reporting>

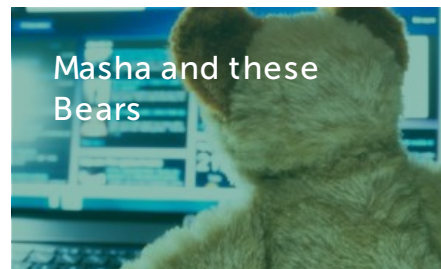
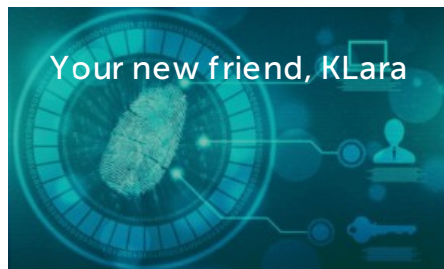
To find more information about cybersecurity awareness training for enterprise or government staff, go to [Kaspersky Security Awareness](#).

APT CYBER ESPIONAGE TARGETED ATTACK

Share post on:



## Related Posts



## LEAVE A REPLY

Your email address will not be published. Required fields are marked \*

Enter your comment here

Name \*

Email \*

Notify me when new comments are added.

SUBMIT



Please upgrade to a [supported browser](#) to get a reCAPTCHA challenge.

Alternatively if you think you are getting this page in error, please check your internet connection and reload.

[Why is this happening to me?](#)

© 2018 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

[Contact us](#) [Privacy Policy](#) [License Agreement](#)

SUBSCRIBE

