Operation Parliament, who is doing what?

securelist.com/operation-parliament-who-is-doing-what/85237/

Authors

GReAT

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.

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

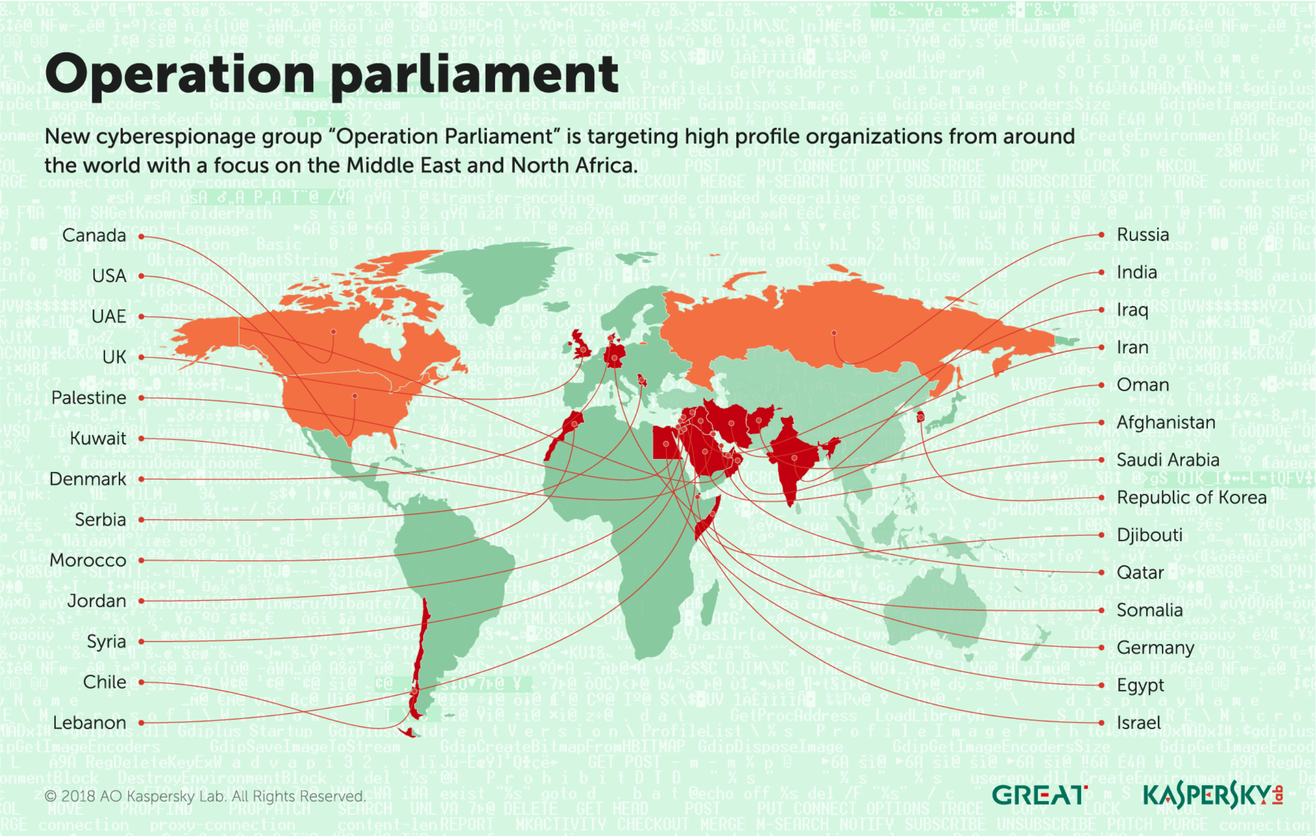
Victimology and Statistics

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.

Victim organization type	Number of victim organizations
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
Distribution/Logistics	1



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

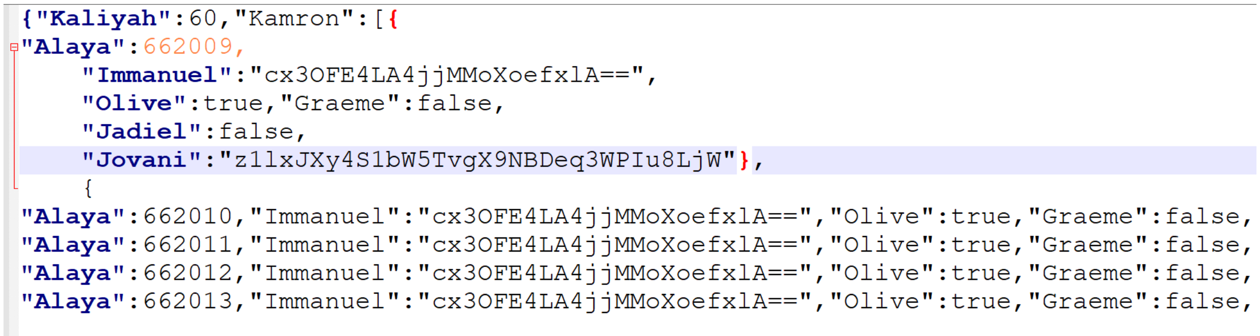
Malware description

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.

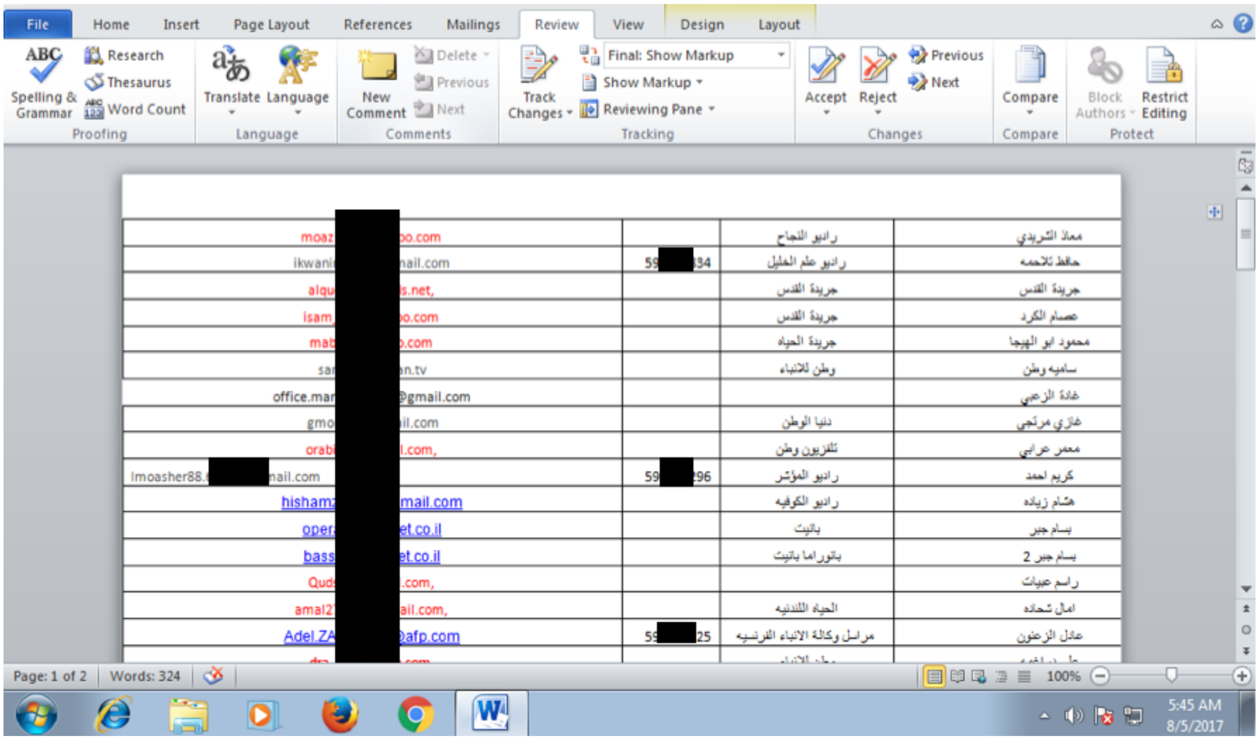
The malware basically provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute scripts/commands and receive the results via HTTP requests.



```
{"Kaliyah":60,"Kamron":[{
"Alaya":662009,
    "Immanuel":"cx3OFE4LA4jjMMoXoefxlA==",
    "Olive":true,"Graeme":false,
    "Jadiel":false,
    "Jovani":"z1lxJXy4S1bW5TvgX9NBDeq3WPIu8LjW"},
    {
"Alaya":662010,"Immanuel":"cx3OFE4LA4jjMMoXoefxlA==","Olive":true,"Graeme":false,
"Alaya":662011,"Immanuel":"cx3OFE4LA4jjMMoXoefxlA==","Olive":true,"Graeme":false,
"Alaya":662012,"Immanuel":"cx3OFE4LA4jjMMoXoefxlA==","Olive":true,"Graeme":false,
"Alaya":662013,"Immanuel":"cx3OFE4LA4jjMMoXoefxlA==","Olive":true,"Graeme":false,
```

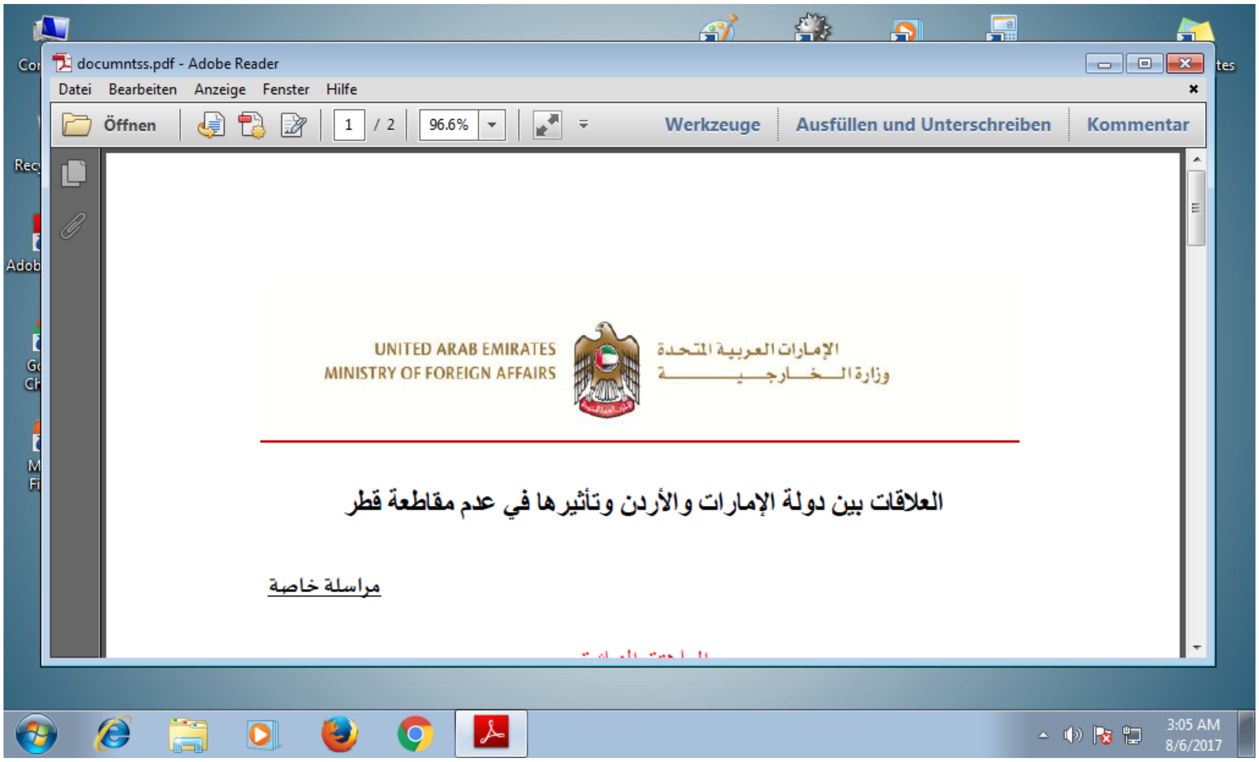
Sample of the C&C response with encrypted commands and configurations

Examples of attack decoys



moaz[redacted]o.com		راديو النجاح	معاذ الشريدي
ikwani[redacted]nail.com	59[redacted]34	راديو علم الخليل	حافظ تلاحمه
alqu[redacted]s.net,		جريدة القدس	جريدة القدس
isam[redacted]o.com		جريدة القدس	عصام الكرد
mab[redacted].com		جريدة الحياة	محمود ابو الهيجا
sa[redacted]n.tv		وطن للانباء	ساميه وطن
office.mar[redacted]@gmail.com			غادة الزعبي
gmo[redacted]il.com		دنيا الوطن	غازي مرتجى
orab[redacted]l.com,		تلفزيون وطن	معمر عرابي
lmoasher88.[redacted]nail.com	59[redacted]96	راديو المؤثر	كريم احمد
hisham[redacted]mail.com		راديو الكوفيه	هشام زياده
oper[redacted]et.co.il		بانيت	بسام جبر
bass[redacted]et.co.il		بانوراما بانيت	بسام جبر 2
Quds[redacted].com,			راسم عبيات
amal2[redacted]ail.com,		الحياه اللندنيه	امال شحاده
Adel.ZA[redacted]@afp.com	59[redacted]25	مراسل وكالة الانباء الفرنسيه	عادل الزعنون
dra[redacted].com		وطن الانباء	[illegible]

Translation: Contacts list of media personnel



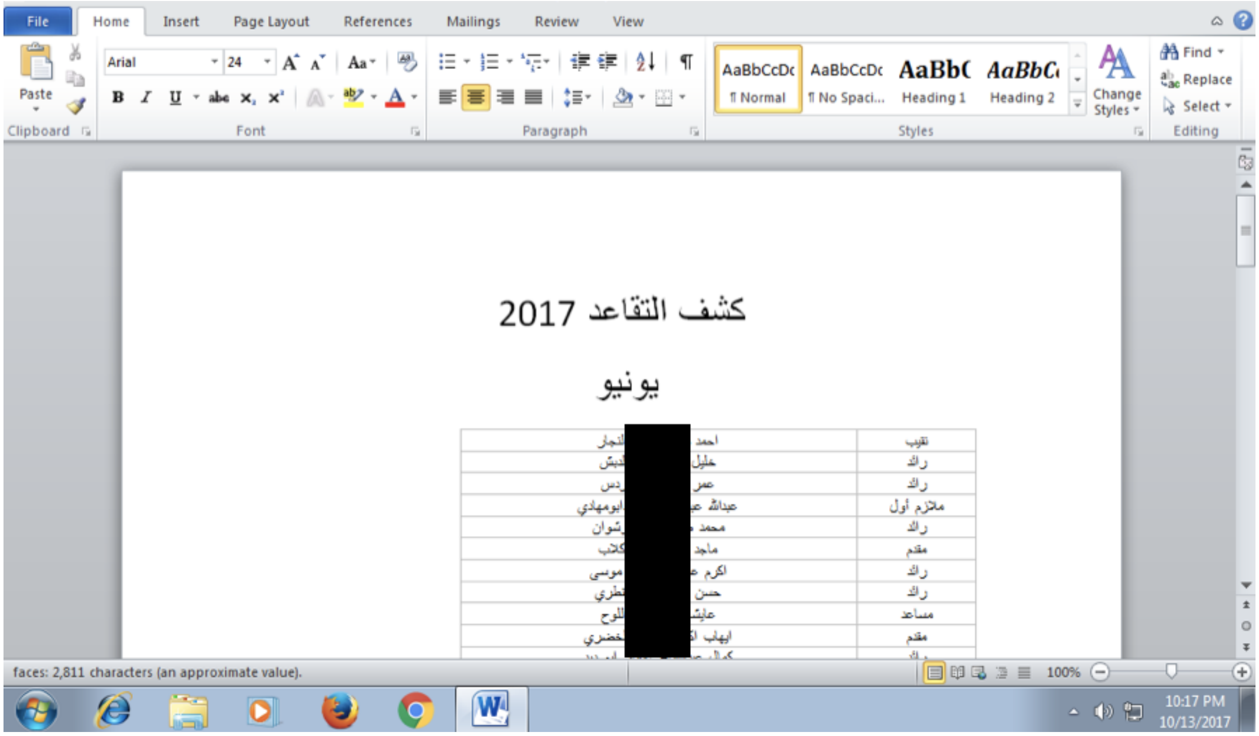
UNITED ARAB EMIRATES
MINISTRY OF FOREIGN AFFAIRS

الإمارات العربية المتحدة
وزارة الخارجية

العلاقات بين دولة الإمارات والأردن وتأثيرها في عدم مقاطعة قطر

مراسلة خاصة

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



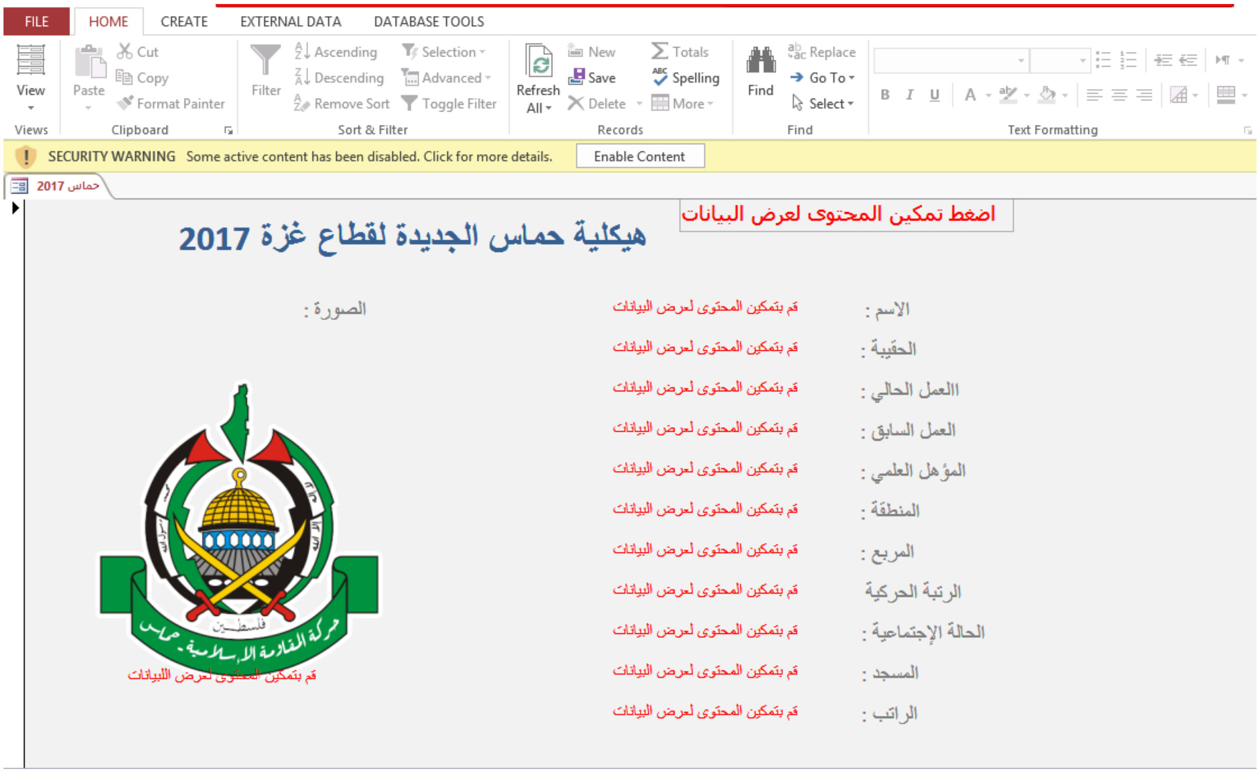
كشف التقاعد 2017

يونيو

احمد [redacted]لتجار	نقيب
خليل [redacted]دبش	رائد
عمر [redacted]ردس	رائد
عبدالله ع[redacted]ابومهادي	ملازم أول
محمد [redacted]رشوان	رائد
ماجد [redacted]كلاب	مقدم
اكرم ع[redacted]موسى	رائد
حسن [redacted]طري	رائد
عايش[redacted]للوح	مساعد
ايهاب ا[redacted]خضري	مقدم

faces: 2,811 characters (an approximate value).

Translation: Military retirement statement 2017 June



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

اضغط تمكين المحتوى لعرض البيانات

هيكلية حماس الجديدة لقطاع غزة 2017

الصورة :

قم بتمكين المحتوى لعرض البيانات

الاسم : قم بتمكين المحتوى لعرض البيانات

الحقيبة : قم بتمكين المحتوى لعرض البيانات

العمل الحالي : قم بتمكين المحتوى لعرض البيانات

العمل السابق : قم بتمكين المحتوى لعرض البيانات

المؤهل العلمي : قم بتمكين المحتوى لعرض البيانات

المنطقة : قم بتمكين المحتوى لعرض البيانات

المربع : قم بتمكين المحتوى لعرض البيانات

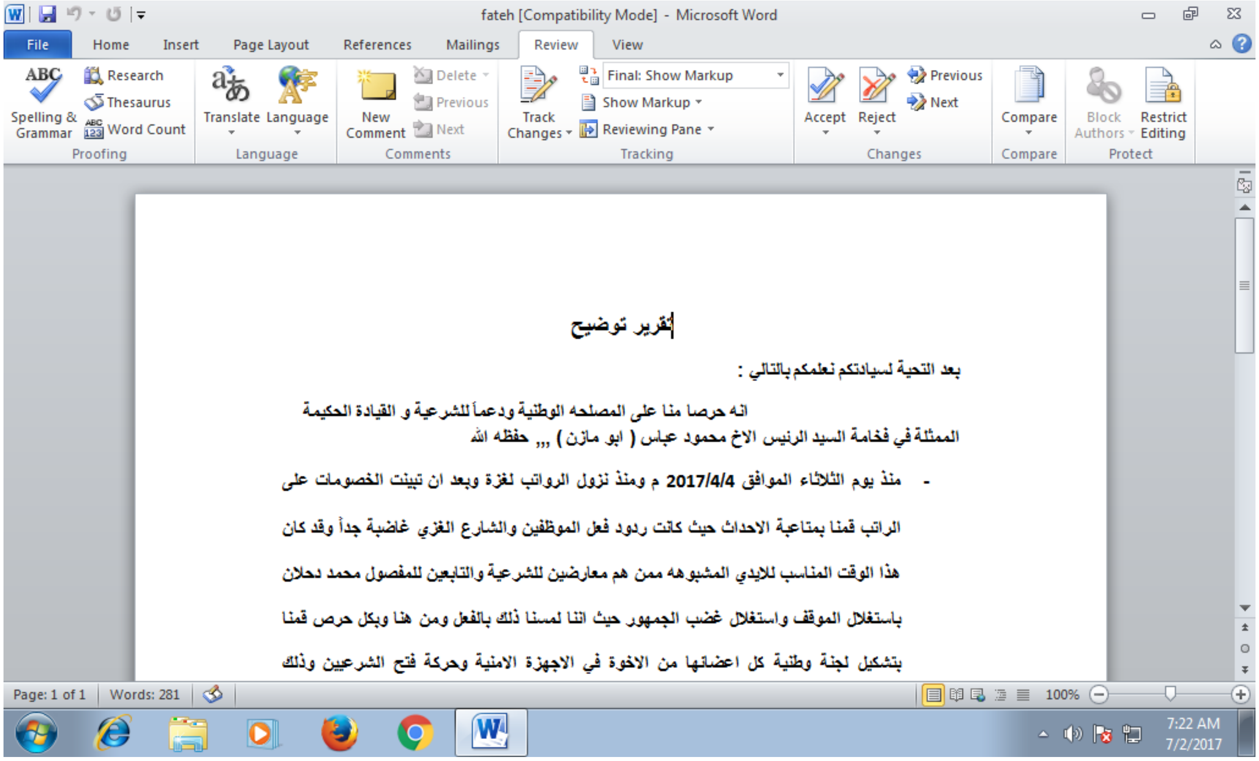
الرتبة الحركية قم بتمكين المحتوى لعرض البيانات

الحالة الإجتماعية : قم بتمكين المحتوى لعرض البيانات

المسجد : قم بتمكين المحتوى لعرض البيانات

الراتب : قم بتمكين المحتوى لعرض البيانات

Translation: The new Hamas structure for Gaza strip 2017



تقرير توضيح

بعد التحية لسيادتكم نعلمكم بالتالي :

انه حرصا منا على المصلحه الوطنية ودعماً للشرعية و القيادة الحكيمة
الممثلة في فخامة السيد الرنيس الاخ محمود عباس (ابو مازن) ,,, حفظه الله

- منذ يوم الثلاثاء الموافق 2017/4/4 م ومنذ نزول الرواتب لغزة وبعد ان تبينت الخصومات على الراتب قمنا بمتاعبة الاحداث حيث كانت ردود فعل الموظفين والشارع الغزي غاضبة جداً وقد كان هذا الوقت المناسب للايدي المشبوهه ممن هم معارضين للشرعية والتابعين للمفصول محمد دحلان باستغلال الموقف واستغلال غضب الجمهور حيث اننا لمسنا ذلك بالفعل ومن هنا وبكل حرص قمنا بتشكيل لجنة وطنية كل اعضائها من الاخوة في الاجهزة الامنية وحركة فتح الشرعيين وذلك

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

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.

Watch Video At:

https://youtu.be/eNpu4ku8tg4

- APT
- Cyber espionage
- Malware Descriptions
- Malware Statistics
- Targeted attacks

Authors

Expert GReAT

Operation Parliament, who is doing what?

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