Operation Molerats: Middle East Cyber Attacks Using Poison Ivy

fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

Don't be too hasty to link every Poison Ivy-based cyber attack to China. The popular remote access tool (RAT), which we recently detailed on this blog, is being used in a broad campaign of attacks launched from the Middle East, too.

First, some background:

In October 2012, malware attacks against Israeli government targets grabbed media attention as officials temporarily cut off Internet access for its entire police force and banned the use of USB memory sticks. [1] Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well. [2] — and as discovered later, even the U.S. and UK governments. [3] Further research revealed a connection between these attacks and members of the so-called "Gaza Hackers Team." We refer to this campaign as "Molerats."

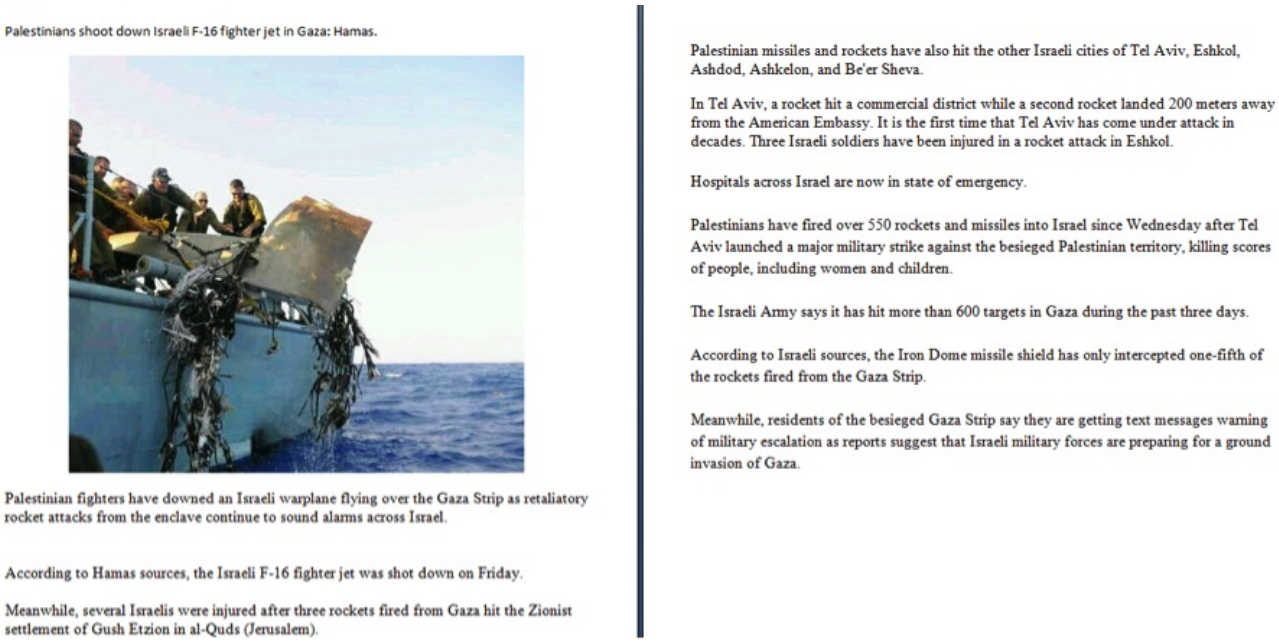
Threat actors in specific geographic regions may prefer one RAT to another, but many RATs are publicly available and used by a variety of threat actors, including those involved in malware-based espionage.

In 2012, the Molerats attacks appeared to rely heavily on the XtremeRAT, a freely available tool that is popular with attackers based in the Middle East. [5] But the group has also used Poison Ivy (PIVY), a RAT more commonly associated with threat actors in China [6] — so much so that PIVY has, inaccurately, become synonymous with all APT attacks linked to China.

This blog post analyzes several recent Molerats attacks that deployed PIVY against targets in the Middle East and in the U.S. We also examine additional PIVY attacks that leverage Arabic-language content related to the ongoing crisis in Egypt and the wider Middle East to lure targets into opening malicious files. [7]

Enter Poison Ivy

We observed several attacks in June and July 2013 against targets in the Middle East and the U.S. that dropped a PIVY payload that connected to command-and-control (CnC) infrastructure used by the Molerats attackers.



Palestinians shoot down Israeli F-16 fighter jet in Gaza: Hamas.

Palestinian fighters have downed an Israeli warplane flying over the Gaza Strip as retaliatory rocket attacks from the enclave continue to sound alarms across Israel.

According to Hamas sources, the Israeli F-16 fighter jet was shot down on Friday.

Meanwhile, several Israelis were injured after three rockets fired from Gaza hit the Zionist settlement of Gush Etzion in al-Quds (Jerusalem).

Palestinian missiles and rockets have also hit the other Israeli cities of Tel Aviv, Eshkol, Ashdod, Ashkelon, and Be'er Sheva.

In Tel Aviv, a rocket hit a commercial district while a second rocket landed 200 meters away from the American Embassy. It is the first time that Tel Aviv has come under attack in decades. Three Israeli soldiers have been injured in a rocket attack in Eshkol.

Hospitals across Israel are now in state of emergency.

Palestinians have fired over 550 rockets and missiles into Israel since Wednesday after Tel Aviv launched a major military strike against the besieged Palestinian territory, killing scores of people, including women and children.

The Israeli Army says it has hit more than 600 targets in Gaza during the past three days.

According to Israeli sources, the Iron Dome missile shield has only intercepted one-fifth of the rockets fired from the Gaza Strip.

Meanwhile, residents of the besieged Gaza Strip say they are getting text messages warning of military escalation as reports suggest that Israeli military forces are preparing for a ground invasion of Gaza.

The malware sample we analyzed was unusual for two reasons:

- It referenced an article that was published last year
- The compile time for the dropped binary was also dated from last year, seemingly consistent with the referenced article. But this malware was signed, and — in contrast to the compile time, which can be faked — the signing time on its certificate was much more recent: Monday, July 08, 2013 1:45:10 A.M.

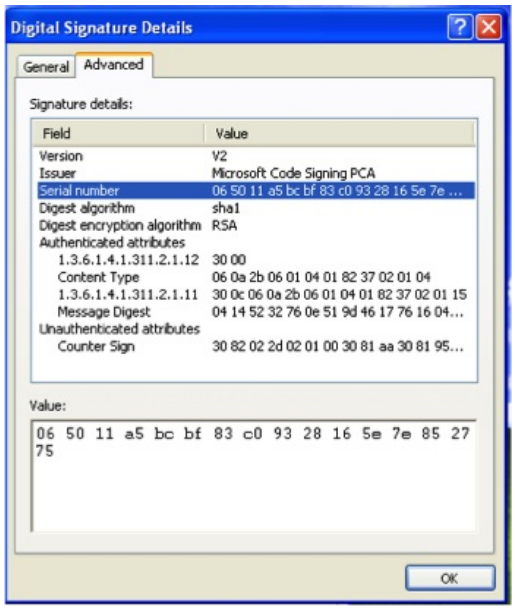
Here are the file details:

Hamas shoot down Israeli F-16 fighter jet by modern weapon in Gaza sea.doc- - - - - - - - - - - .scr

`MD5: 7084f3a2d63a16a191b7fcb2b19f0e0d`

This malware was signed with a forged Microsoft certificate similar to previous XtremeRat samples. But the serial number (which is often reused by attackers, enabling FireEye researchers to link individual attacks, including those by the Molerats) is different this time.

The malware dropped an instance of PIVY with the following configuration:



ID: F16 08-07-2013

Group:

DNS/Port: Direct: toornt.servegame.com:443,

Proxy DNS/Port:

Proxy Hijack: No

ActiveX Startup Key:

HKLM Startup Entry:

File Name:

Install Path: C:\Documents and Settings\Admin\Local Settings\Temp\morse.exe

Keylog Path: C:\Documents and Settings\Admin\Local Settings\Temp\morse

Inject: No

Process Mutex: gdfgdfgdg

Key Logger Mutex:

ActiveX Startup: No

HKLM Startup: No

Copy To: No

Melt: No

Persistence: No

Keylogger: No

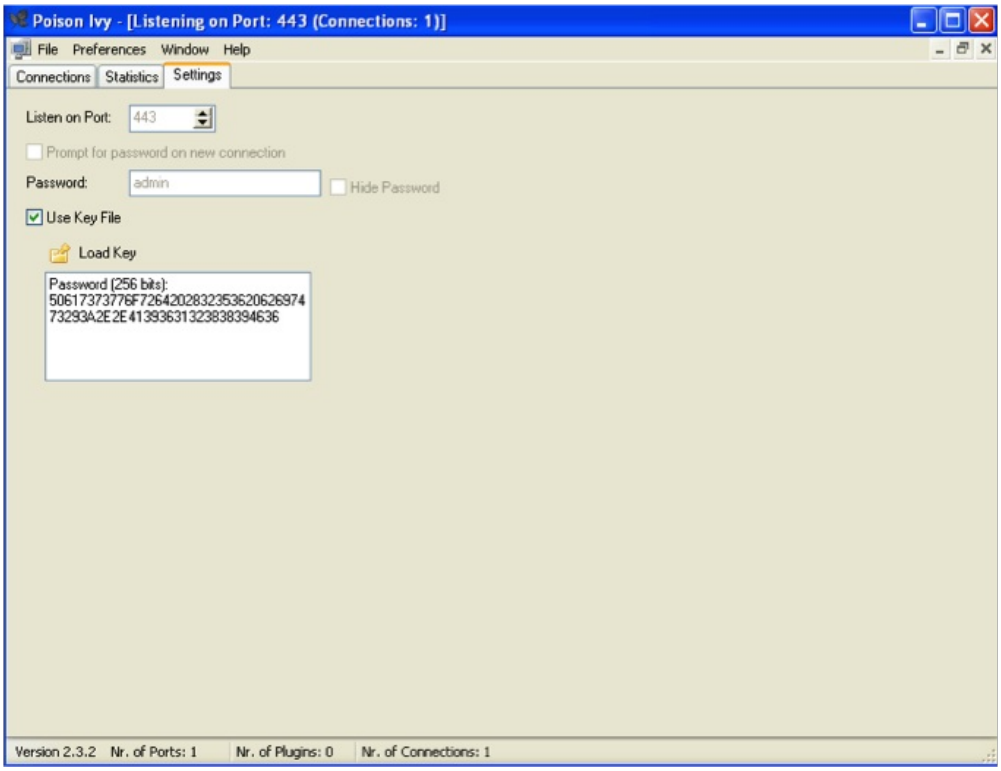
Password: !@#GooD#@!

We collected additional PIVY samples that had the same password or linked to CnC infrastructure at a common IP address (or both). We observed three PIVY passwords (another potential identifier) used in the attacks: “!@#GooD#@!”, “!@#Goood#@!” and “admin100”.

Additional Samples with Middle Eastern Themes

We also found a PIVY sample used by this group that leveraged what are known as key files instead of passwords. The PIVY builder allows operators to load .pik files containing a key to secure communications between the compromised computer and the attacker's machine. By default, PIVY secures these communications with the ascii text password of "admin" — when the same non-default password appears in multiple attacks, researchers can conclude that the attacks are related.

The PIVY sample in question had an MD5 hash of 9dff139bbbe476770294fb86f4e156ac and communicated with a CnC server at toornt.servegame.com over port 443. The key file used to secure communications contained the following ascii string ‘Password (256 bits):\x0d\x0aA9612889F6’ (where \x0d\x0a represents a line break).



The 9dff139bbbe476770294fb86f4e156ac sample dropped a decoy document in Arabic that included a transcript of an interview with Salam Fayyad, the former Prime Minister of the Palestinian National Authority.

The sample 16346b95e6deef9da7fe796c31b9dec4 was also seen communicating with toornt.servegame.com over port 443. This sample appears to have been delivered to its targets via a link to a RAR archive labeled *Ramadan.rar* (fc554a0ad7cf9d4f47ec4f297dbde375) hosted at the Dropbox file-sharing website.

نبذة

يذكر ان الفريق اول السيسي مولود العام 1954 ومن مؤهلاته: بكالوريوس العلوم العسكرية عام 1977، ماجستير العلوم العسكرية من كلية القادة والأركان عام 1987، ماجستير العلوم العسكرية من كلية القادة والأركان البريطانية عام 1992، زمالة كلية الحرب العليا من أكاديمية ناصر العسكرية العليا عام 2003 ، زمالة كلية الحرب العليا الأميركية عام 2006.

وكان الفريق اول أصغر أعضاء المجلس الأعلى للقوات المسلحة سنًا قبل اختياره لمنصبه، وتولى قبل ذلك مهام: رئيس فرع المعلومات والأمن بالأمانة العامة لوزارة الدفاع، قائد كتيبة مشاة ميكانيكي، ملحق دفاع بالمملكة العربية السعودية، قائد لواء مشاة ميكانيكي، قائد فرقة مشاة ميكانيكي)الفرقة الثانية)، رئيس أركان المنطقة الشمالية العسكرية، قائد المنطقة الشمالية العسكرية ومدير إدارة المخابرات الحربية والاستطلاع

إرادة الشعب

وما خطف الانتباه بالنسبة لرجل مصر القوي هو رده غير مباشر على تهديدات قيادات اسلامية بالتصدي بالقوة لتظاهرات 30 حزيران (يونيو) الماضي، حيث كان السيسي أكد في تصريحات علنية في 24 يونيو انحياز الجيش "لإرادة الشعب"، وقال إن "الموت أشرف لنا من ان يمس أحد من شعب مصر في وجود جيشه"، مضيفا "ليس من المروءة ان نصمت أمام تخويف وترويع أهالينا المصريين."

مواقف السيسي

The sample a8714aac274a18f1724d9702d40030bf dropped a decoy document in Arabic that contained a biography of General Adbel Fattah el-Sisi – the Commander-in-Chief of the Egyptian Armed Forces.

ورطة السيسي والوطن

مما لا شك فيه ان السيسي وضع نفسه والمؤسسة العسكرية في ورطة لا يحسد عليها..

صلاح محفوظ

قبل ان نتحدث عن ورطة السيسي نرجع بشريط الاحداث قليلا الى الوراء نعود الى نهاية يوم مظاهرات الثورة المضادة امام الاتحادية و في ميدان التحرير سابقا ؛ كانت فعاليات غضبة القلول قد انتهت بعد ان اصابهم الرعب من حشود مؤيدي الرئيس في رابعة العدوية ومع ساعات الصباح الاولى انصرف المأجورين من البلطجية وعاد القساوسة الى كنائسهم والقلول الى جحورهم..

الا ان السيسي الذي رتب للانقلاب على الشرعية بعد ان غازله معتصمي وزارة الدفاع بقولهم سيسي يا سيسي انت رئيسي ولعبت احلام الرئاسة بخياله.

ولا اعرف كيف آمن له محمد مرسي بعد ان استخدمه في الانقلاب على العشير طنطاوي؛ فهو اذا شخصية انقلابية.

كانت الحشود التابعة للثورة المضادة قد بدأت في الانصراف فلم يرض هذا طموحات السيسي فاصدر بيان الجيش رقم واحد ومنح الجميع مهلة 48 ساعة تنتهي اليوم اي انه طلب من القلول الانتظار 48 ساعة اضافية حتى يستطيع اخراج مشهد الانقلاب بأقل الخسائر خاصة وهو يعلم ان سياسة الانقلابات انتهت منذ زمن في كثير من دول العالم واصبح المجتمع الدولي لا يدعمها

السيسي لم يجيد قراءة المشهد وتوهم انه قادر على اللعب بالنار مستدلا حشد النصارى والقلولوم يضع في حساباته ان الرئيس اتى عبر صندوق الانتخاب وان الملايين من الشعب المصري من غير المنتمين للتيار الاسلامي والاخوان لن يقبلوا ابدا الانقضاض على الثورة ولم يضع السيسي في حساباته ان الحشد المسيحي الكنسي في ميدان التحرير استفز غالبية الشعب المصري فنزلوا بحشود غير مسبوقة لم تراها مصر من قبل.

وهنا وامام هذا الحشود يقف السيسي محاصرا بين حشود لا قبل له بها وبين انذار ندم على توجيهه او تسرع في اعلانه ولا يعرف ماذا يفعل الان ؟

السيناريوهات المتاحة امامه وفق المعطيات على الارض :

1- **اعلان عزل رئيس الجمهورية وهنا تبدأ الثورة الاسلامية والحرب الاهلية ويتكرر السيناريو السوري ولا اعتقد ان السيسي غبي الى هذا الحد ليقدم على هذا الفعل ويغامر بمستقبله ومصير مصر وجيشها**

2- **اعلان خارطة طريق مرفوضة من التيار الاسلامي والشعبي ستطيل عمر الازمة**

3- **الانحياز للشرعية والاحتكام الى اعداد المتظاهرين على الارض.**

A recent sample (d9a7c4a100cfefef995785f707be895c) used protests in Egypt to entice recipients to open a malicious file.

بالصور : اعتصامات الإخوان أصبحت مورد للسلوك للجماعة

منذ بداية الاعتصامات واستقرار المتظاهرين في الميادين بدأ تأثر الناس وإقبالهم على البضاعة التي يقدمها الإخوان لكل من يحضر للميدان من جميع أطياف الشعب المصري والوافدين من جميع أقطار مصر الحبيبة ومن أهم تلك السلع والبضائع هو نشر الدين الإسلامي وتعاليمه وتوضيح طريق الخير للناس المغيبة والمضللة من الإعلام المصري الخبيث

وفي اطار آخر بدأ كثير من الناس بالحضور للميادين لسماع الصوت الندي في قراءة القرآن ....

Another sample (b0a9abc76a2b4335074a13939c59bfc9) contained a decoy with a grim picture of Fadel Al Radfani, who was the adviser to the defense minister of Yemen before he was assassinated.

Although we are seeing Egyptian- and Middle Eastern-themed attacks using decoy content in Arabic, we cannot determine the intended targets of all of these attacks.

Delivery Vector

We believe that the Molerats attacker uses spear phishing to deliver weaponized RAR files containing their malicious payloads to their victims in at least two different ways. The Molerats actor will in some cases attach the weaponized RAR file directly to their spear- phishing-emails. We also believe that this actor sends spear-phishing emails that include links to RAR files hosted on third-party platforms such as Dropbox.

In one such example we found the following link was used to host *Ramadan.rar* (fc554a0ad7cf9d4f47ec4f297dbde375):

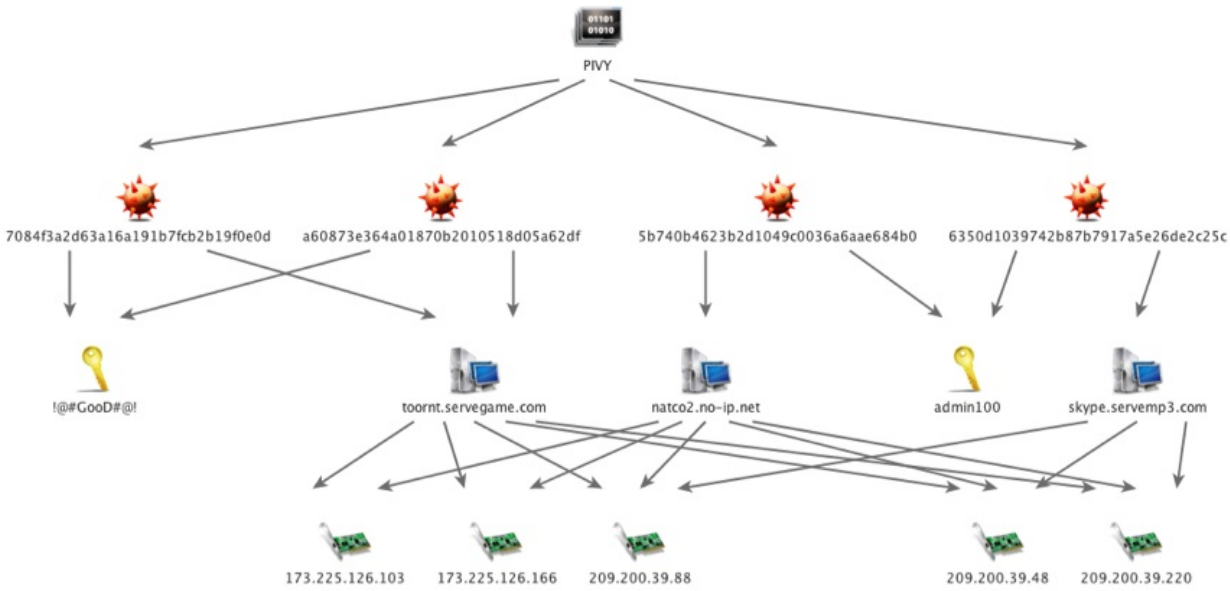
hxxps://dl[.]dropboxusercontent[.]com/s/uiod7orcpykx2g8/Ramadan.rar?token_hash=AAHAVuiXpTkOKwar9e0WH-EfrK7PEB9O7t7WC6Tgtn315w&dl=1

CnC Infrastructure

We have found 15 PIVY samples that can be linked through common passwords, common CnC domain names, and common IP addresses to which the CnC domains resolve. The CnC servers for this cluster of activity are:

- toornt.servegame.com
- updateo.servegame.com
- egypttv.sytes.net
- skype.servemp3.com
- natco2.no-ip.net

Two of the domain names (natco2.no-ip.net and skype.servemp3.com) that were used as CnCs for PIVY were both documented as XtremeRat CnCs that were used in previous attacks. [8]



We focused on these domains and their IP addresses — which they had in common with toornt.servegame.com. In addition, we added the well-known CnCs good.zapto.org and hint.zapto.org used in previously documented attacks.

By observing changes in DNS resolution that occurred within the same timeframe, we were able to ensure that the passive DNS data we collected was the same. Interestingly, we also found that the domains often shifted to a new IP address over time.

CnC	Date	IP
toornt.servegame.comnatco2.no-ip.netskype.servemp3.comgood.zapto.orghint.zapto.org		209.200.39.48
toornt.servegame.comnatco2.no-ip.netskype.servemp3.comgood.zapto.orghint.zapto.org		209.200.39.88
toornt.servegame.comnatco2.no-ip.nethint.zapto.org		173.225.126.166
toornt.servegame.comnatco2.no-ip.net		173.225.126.103
toornt.servegame.comnatco2.no-ip.netskype.servemp3.comgood.zapto.orghint.zapto.org		209.200.39.220

natco2.no-ip.netgood.zapto.orghint.zapto.orgtoornt.servegame.comomagle.serveblog.netskype.servemp3.com	209.200.39.48
egypttv.sytes.nettoornt.servegame.com	173.225.126.179

One interesting discovery concerns a sample (5b740b4623b2d1049c0036a6aae684b0) that was first seen by VirusTotal on September 14, 2012. This date is within the timeframe of the original XtremeRat attacks, but the payload in this case was PIVY. This indicates that the attackers have been using PIVY in addition to XtremeRat for longer than we had originally believed.

Conclusion

We do not know whether using PIVY is an attempt by those behind the Molerats campaign to frame China-based threat actors for their attacks or simply evidence that they have added another effective, publicly-available RAT to its arsenal. But this development should raise a warning flag for anyone tempted to automatically attribute all PIVY attacks to threat actors based in China. The ubiquity of off-the-shelf RATs makes determining those responsible an increasing challenge.

The ongoing attacks are also heavily leveraging content in Arabic that uses conflicts in Egypt and the wider Middle East to lure targets into opening malicious files. But we have no further information about the exact targets of these Arabic lures.

As events on the ground in the Middle East — and in Egypt in particular — receive international attention, we expect the Molerat operators to continue leveraging these headlines to catalyze their operations.

Notes

1. http://www.timesofisrael.com/how-israel-police-computers-were-hacked-the-inside-story/ http://www.haaretz.com/blogs/diplomania/israel-s-foreign-ministry-targeted-by-computer-virus-bearing-idf-chief-s-name.premium-1.472278

2. http://download01.norman.no/whitepapers/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

3. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/

4. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/

5. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/

6. /content/dam/legacy/resources/pdfs/fireeye-poison-ivy-report.pdf

7. The Molerats group also uses addition RATs such as XtremeRat, Cerberus, Cybergate, but we have focused on their used of PIVY in this blog.

8. http://download01.norman.no/whitepapers/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

Yara Signature

This Yara signature can be used to locate signed samples that have the new certificate serial numbers used by Molerats.

```
rule Molerats_certs
{
meta:
author = “FireEye Labs”
description = “this rule detections code signed with certificates used by the Molerats actor”
strings:
$cert1 = {06 50 11 A5 BC BF 83 C0 93 28 16 5E 7E 85 27 75}
$cert2 = {03 e1 e1 aa a5 bc a1 9f ba 8c 42 05 8b 4a bf 28}
$cert3 = {0c c0 35 9c 9c 3c da 00 d7 e9 da 2d c6 ba 7b 6d}
condition:
```

```
1 of ($cert*)
```

```
}
```

Samples

9dff139bbbe476770294fb86f4e156ac

6350d1039742b87b7917a5e26de2c25c

b0a9abc76a2b4335074a13939c59bfc9

5b740b4623b2d1049c0036a6aae684b0

9dff139bbbe476770294fb86f4e156ac

cf31aea415e7013e85d1687a1c0f5daa

973b5f2a5608d243e7305ee4f9249302

e85fc76362c2e9dc7329fddda8acc89e

b05603938a888018d4dcdc551c4be8ac

7084f3a2d63a16a191b7fcb2b19f0e0d

16346b95e6deef9da7fe796c31b9dec4

a8714aac274a18f1724d9702d40030bf

d9a7c4a100cfefef995785f707be895c

9ef9a631160b96322010a5238defc673

a60873e364a01870b2010518d05a62df