Molerats, Here for Spring!

fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html

Between 29 April and 27 May, FireEye Labs identified several new Molerats attacks targeting at least one major U.S. financial institution and multiple, European government organizations.

When we last published details relevant to Molerats activity in August of 2013, we covered a large campaign of Poison Ivy (PIVY) attacks directed against several targets in the Middle East and the United States. We felt it was significant to highlight the previous PIVY campaigns to:

- Demonstrate that any large-scale, targeted attacks utilizing this off-the-shelf Remote Access Tool (RAT) shouldn't be automatically linked to Chinese threat actors.
- Share several documented tactics, techniques, and procedures (TTP), and indicators of compromise (IOC) for identifying Molerats activity.

However, this was just one unique facet to a much broader series of related attacks dating back to as early as October 2011 and are still ongoing. Previous research has linked these campaigns to Molerats, but with so much public attention focused on APT threat actors based in China, it's easy to lose track of targeted attacks carried out by other threat actor

groups based elsewhere. For example, we recently published the "Operation Saffron Rose" whitepaper, detailing a rapidly evolving Iranian-based threat actor group known as the “Ajax Security Team."

New Attacks, Same Old Tactics

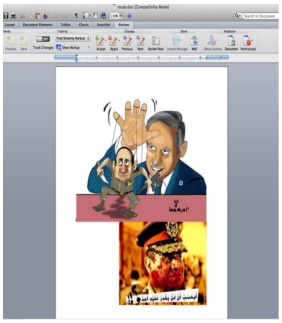
With the reuse of command and control (CnC) infrastructure and a similar set of TTPs, Molerats activity has been tracked and expanded to a growing target list, which includes:

- Palestinian and Israeli surveillance targets
- Government departments in Israel, Turkey, Slovenia, Macedonia, New Zealand, Latvia, the U.S., and the UK
- The Office of the Quartet Representative
- The British Broadcasting Corporation (BBC)
- A major U.S. financial institution
- Multiple European government organizations

Previous Molerats campaigns have used several garden-variety, freely available backdoors such as CyberGate and Bifrost, but, most recently, we have observed them making use of the PIVY and Xtreme RATs. Previous campaigns made use of at least one of three observed forged Microsoft certificates, allowing security researchers to accurately tie together separate attacks even if the attacks used different backdoors. There also appears to be a habitual use of lures or decoy documents – in either English or Arabic-language – with content focusing on active conflicts in the Middle East. The lures come packaged with malicious files that drop the Molerats’ flavor of the week, which happen to all be Xtreme RAT binaries in these most recent campaigns.

Groundhog Day

On 27 May we observed at least one victim downloading a malicious .ZIP file as the result of clicking on a shortened Google URL – http://goo[.]gl[/]AMD3yX – likely contained inside of a targeted spearphishing email. However, we were unable to confirm for this particular victim:

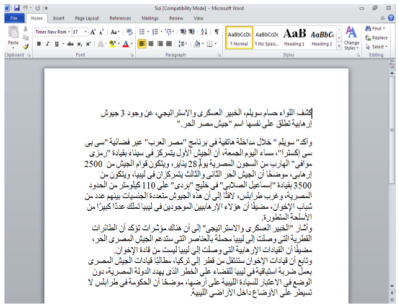


1) “حصري بالصور لحظة الإعتداء على المشير عبد الفتاح السيسي.scr” (MD5: a6a839438d35f503dfebc6c5eec4330e)

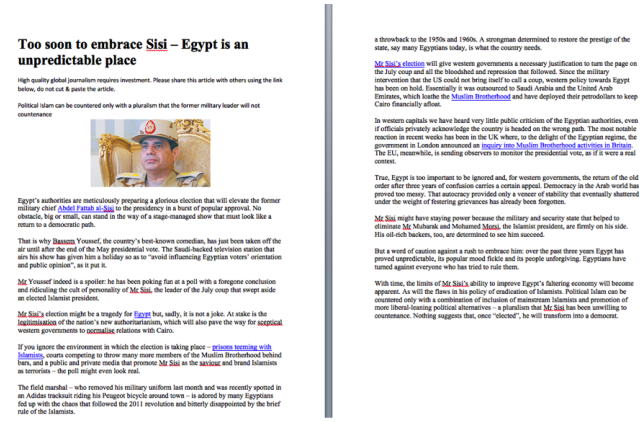
- Malicious download URL was sent to a well-known European government organization.
- The shortened URL breaks out to “http://lovegame[.]us/ Photos[.]zip,” which was clicked/downloaded by the victim.
- The extracted binary, “حصري بالصور لحظة الإعتداء على المشير عبد الفتاح السيسي.scr,” opens up a decoy Word document and installs/executes the Xtreme RAT binary into a temp directory, “Documents and Settings\admin\Local Settings\Temp\Chrome.exe.”
- The decoy document, “rotab.doc,” contains three images (a political cartoon and two edited photos), all negatively depicting former military chief Abdel Fattah el-Sisi.
- Xtreme RAT binary dropped: “Chrome.exe” (MD5: a90225a88ee974453b93ee7f0d93b104), which is unsigned.
- As of 29 May, the URL has been clicked 225 times by a variety of platforms and browser types, so the campaign was likely not limited to just one victim.
- Two of the download referrers are webmail providers (EIM.ae” and “Sltnet.lk”) further indicating the malicious URL was likely disseminated via spearphishing emails.

On 29 April we observed two unique malicious attachments being sent to two different victims via spearphishing emails:

2) 8ca915ab1d69a7007237eb83ae37eae5



- Malicious file sent to both the financial institution and Ministry of Foreign Affairs targets.
- Drops an Arabic language decoy document titled “Sisi.doc”, which appears to contain several copy/pasted excerpts of (now retired) Egyptian Major General Hossam Sweilem, discussing military strategy and the Muslim Brotherhood.
- The title of the document appears to have several Chinese characters, yet the entire body of the document is written in Arabic. As noted in our August 2013 blog post, this could possibly be a poor attempt to frame China-based threat actors for these attacks.
- Xtreme RAT binary dropped: “sky.exe” (MD5: 2d843b8452b5e48acbbe869e51337993), which is unsigned.



Too soon to embrace Sisi – Egypt is an unpredictable place

High quality global journalism requires investment. Please share this article with others using the link below, do not cut & paste the article.

Political Islam can be countered only with a pluralism that the former military leader will not countenance

Egypt's authorities are meticulously preparing a glorious election that will elevate the former military chief Abdel Fattah al-Sisi to the presidency in a burst of popular approval. No obstacle, big or small, can stand in the way of a stage-managed show that must look like a return to a democratic path.

That is why Bassem Youssef, the country's best-known comedian, has just been taken off the air until after the end of the May presidential vote. The Saudi-backed television station that airs his show has given him a holiday so as to "avoid influencing Egyptian voters' orientation and public opinion", as it put it.

Mr Youssef indeed is a spoiler: he has been poking fun at a poll with a foregone conclusion and ridiculing the cult of personality of Mr Sisi, the leader of the July coup that swept aside an elected Islamist president.

Mr Sisi's election might be a tragedy for Egypt but, sadly, it is not a joke. At stake is the legitimisation of the nation's new authoritarianism, which will also pave the way for sceptical western governments to normalise relations with Cairo.

If you ignore the environment in which the election is taking place – prisons teeming with Islamists, courts competing to throw many more members of the Muslim Brotherhood behind bars, and a public and private media that promote Mr Sisi as the saviour and brand Islamists as terrorists – the poll might even look real.

The field marshal – who removed his military uniform last month and was recently spotted in an Adidas tracksuit riding his Peugeot bicycle around town – is adored by many Egyptians fed up with the chaos that followed the 2011 revolution and bitterly disappointed by the brief rule of the Islamists.

a throwback to the 1950s and 1960s. A strongman determined to restore the prestige of the state, say many Egyptians today, is what the country needs.

Mr Sisi's election will give western governments a necessary justification to turn the page on the July coup and all the bloodshed and repression that followed. Since the military intervention that the US could not bring itself to call a coup, western policy towards Egypt has been on hold. Essentially it was outsourced to Saudi Arabia and the United Arab Emirates, which loathe the Muslim Brotherhood and have deployed their petrodollars to keep Cairo financially afloat.

In western capitals we have heard very little public criticism of the Egyptian authorities, even if officials privately acknowledge the country is headed on the wrong path. The most notable reaction in recent weeks has been in the UK where, to the delight of the Egyptian regime, the government in London announced an inquiry into Muslim Brotherhood activities in Britain. The EU, meanwhile, is sending observers to monitor the presidential vote, as if it were a real contest.

True, Egypt is too important to be ignored and, for western governments, the return of the old order after three years of confusion carries a certain appeal. Democracy in the Arab world has proved too messy. That autocracy provided only a veneer of stability that eventually shattered under the weight of festering grievances has already been forgotten.

Mr Sisi might have staying power because the military and security state that helped to eliminate Mr Mubarak and Mohamed Morsi, the Islamist president, are firmly on his side. His oil-rich backers, too, are determined to see him succeed.

But a word of caution against a rush to embrace him: over the past three years Egypt has proved unpredictable, its popular mood fickle and its people unforgiving. Egyptians have turned against everyone who has tried to rule them.

With time, the limits of Mr Sisi's ability to improve Egypt's faltering economy will become apparent. As will the flaws in his policy of eradication of Islamists. Political Islam can be countered only with a combination of inclusion of mainstream Islamists and promotion of more liberal-leaning political alternatives – a pluralism that Mr Sisi has been unwilling to countenance. Nothing suggests that, once "elected", he will transform into a democrat.

3) “Too soon to embrace Sisi _ Egypt is an unpredictable place.scr" (MD5: 7f9c06cd950239841378f74bbacbef60)

- Malicious file only sent to a European government organization.
- Drops an English language decoy document also titled “Sisi.doc”, however this one appears to be an exact copy of a 23 April Financial Times’ news article about the uncertainties surrounding former military chief Abdel Fattah el-Sisi running for president in the upcoming Egyptian elections.
- Drops the same Xtreme RAT binary: “sky.exe” (MD5: 2d843b8452b5e48acbbe869e51337993), which is unsigned.

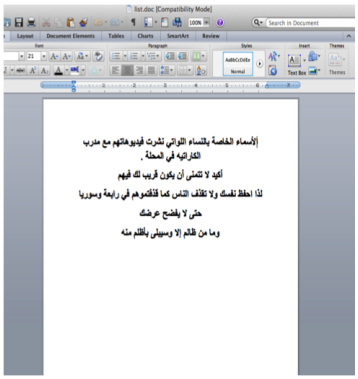
Another attribute regularly exhibited by Molerats malware samples are that they are often archived inside of self-extracting RAR files and encoded with EXECryptor V2.2, along with several other legitimate looking archived files.

Related Samples

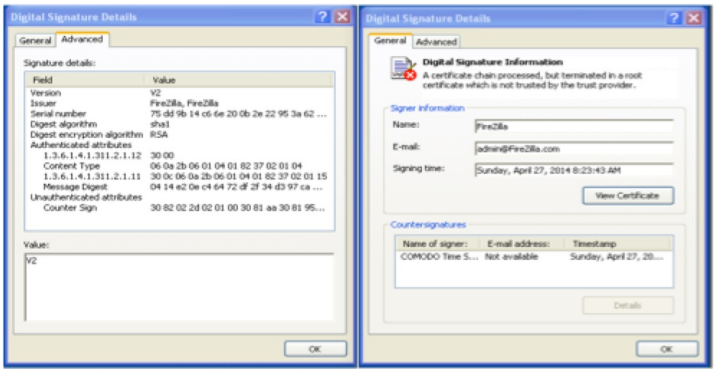
Both of the malicious files above have a compile date/time of **2014-04-17 09:43:29-0000,** and, based on this information, we were able to identify five additional samples (one sample only contained a lure but no malicious binary), related to the 29 April attacks. These samples were a little more interesting, because they contained an array of either attempted forged or self-signed Authenticode certificates.

All of the additionally identified samples were sent to one of the same European government organizations mentioned previously.

4) 2b0f8a8d8249402be0d83aedd9073662

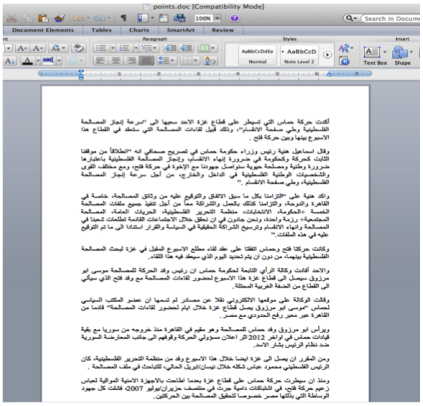


- Drops an Arabic language Word Document titled “list.doc”.
- The title of the document appears to have several Chinese characters, yet the entire body of the document is written in Arabic.
- Xtreme RAT binary dropped: “Download.exe” (MD5: cff48ff88c81795ee8cebdc3306605d0). This malware is signed with a self-signed certificate issued by “FireZilla” (see below).Certificate serial number: {75 dd 9b 14 c6 6e 20 0b 2e 22 95 3a 62 7b 39 19}.

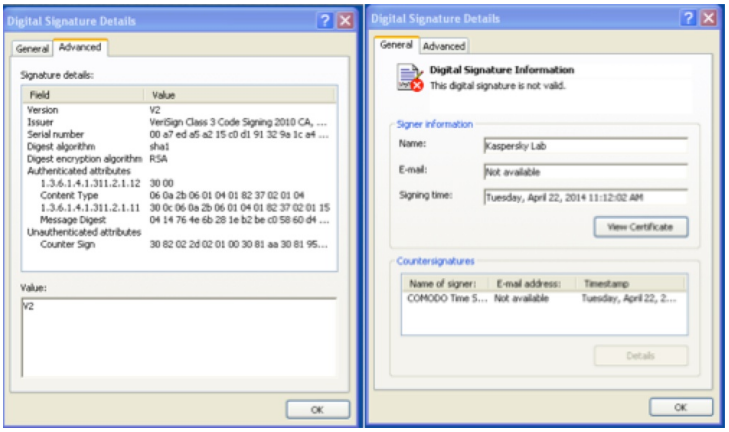


Forged FireZilla certificate

5) 4f170683ae19b5eabcc54a578f2b530b



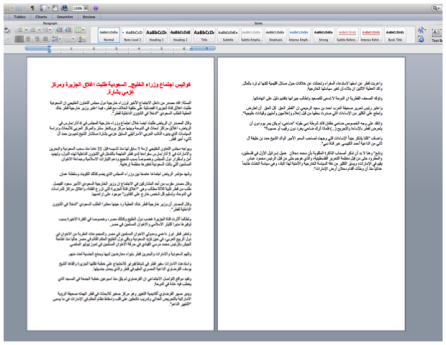
- Drops an Arabic language Word Document titled “points.doc,” which appears to be an online clipping from a news article about ongoing Palestinian reconciliation meetings between Fatah and Hamas in the Gaza strip.
- The title of the document appears to have several Chinese characters, yet the entire body of the document is written in Arabic.
- Xtreme RAT binary dropped: “VBB.exe” (MD5: 6f9585c8748cd0e7103eab4eda233666). Though the malware appeared to be signed with a certificate named “Kaspersky Lab”, the real hash did not match the signed hash (see below).Certificate serial number: {a7 ed a5 a2 15 c0 d1 91 32 9a 1c a4 b0 53 eb 18}.



(Forged Kaspersky Lab certificate)

6) 793b7340b7c713e79518776f5710e9dd & a75281ee9c7c365a776ce8d2b11d28da

- Both drop an Arabic language Word Document titled “qatar.doc,” which appears to be an online clipping for a new article concerning members of the Gulf Cooperation Council (GCC) and the ongoing conflicts between Saudi Arabia, the United Arab Emirates (UAE), and Bahrain – all against Qatar because of the country’s support for the Muslim Brotherhood.
- The title of the document appears to have several Chinese characters, yet the entire body of the document is written in Arabic.
- Xtreme RAT binary dropped by the first sample: “AVG.exe” (MD5: a51da465920589253bf32c6115072909), which is unsigned.



7) Pivoting off one of the fake Authenticode certificates we were able to identify at least one additional related binary, “vmware.exe” (MD5: 6be46a719b962792fd8f453914a87d3e), also Xtreme RAT, but doesn’t appear to have been sent to any of our customers. The malicious binary is also encoded with EXECryptor V2.2–similar to the samples above–and the CnC domain has resolved to IPs that overlap with previously identified Molerats malware.

Indicators of Compromise

MD5	Callback URLs
8ca915ab1d69a7007237eb83ae37eae5	http://www.uae[.]kim:81/12345000[.]functions
7f9c06cd950239841378f74bbacbef60	http://www.uae[.]kim:81/12345000[.]functions
2b0f8a8d8249402be0d83aedd9073662	http://www.uae[.]kim:8888/1411[.]functions
4f170683ae19b5eabcc54a578f2b530b	http://updato.systes[.]net:3398/1411[.]functions
793b7340b7c713e79518776f5710e9dd	http://removalmalware.servecounterstrike[.]com:443/12345000[.]functions **(NON-SSL)**
6be46a719b962792fd8f45391 4a87d3e	http://mailchat.zapto[.]org:8008/81018[.]functions
a6a839438d35f503dfebc6c5eec4330e	http://updato.sytes[.]net:35001/12345000[.]functions

Although the samples above are all Xtreme RAT, all but two samples communicate over different TCP ports. The port 443 callback listed in the last sample is also not using actual SSL, but instead, the sample transmits communications in clear-text – a common tactic employed by adversaries to try and bypass firewall/proxy rules applying to communications over traditional web ports. These tactics, among several others mentioned previously, seem to indicate that Molerats are not only aware of security researchers’ efforts in trying to track them but are also attempting to avoid using any obvious, repeating patterns that could be used to more easily track endpoints infected with their malware.

Conclusion

Although a large number of attacks against our customers appear to originate from China, we are tracking lesser-known actors also targeting the same firms. Molerats campaigns seem to be limited to only using freely available malware; however, their growing list of targets and increasingly evolving techniques in subsequent campaigns are certainly noteworthy.

MD5 Samples

- a6a839438d35f503dfebc6c5eec4330e
- 7f9c06cd950239841378f74bbacbef60
- 8ca915ab1d69a7007237eb83ae37eae5
- 2b0f8a8d8249402be0d83aedd9073662
- 4f170683ae19b5eabcc54a578f2b530b
- 793b7340b7c713e79518776f5710e9dd
- a75281ee9c7c365a776ce8d2b11d28da
- 6be46a719b962792fd8f453914a87d3e

Older Molerats samples from Dec 2013 (not listed above)

- 34c5e6b2a988076035e47d1f74319e86
- 13e351c327579fee7c2b975b17ef377c
- c0488b48d6aabe828a76ae427bd36cf1
- 14d83f01ecf644dc29302b95542c9d35

References & Credits

A special thanks to Ned Moran and Matt Briggs of FireEye Labs for supporting this research.

- https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
- http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/
- http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf