Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International.

This issue is for your personal use only.

Published monthly in Russian and in English
by *Trialogue Company Ltd.*

Issue № 9, vol.2. September 2012.

September 5, 2012

Oleg Demidov, Maxim Simonenko report from Moscow:

FLAME IN CYBERSPACE

ANNOTATION

It is not Iran that the story of Flame begins with. The first versions of this malware, or rather of its prototype, were found by the American company Webroot Community in late 2007 in Europe. The following year the virus was spotted in the UAE. At the time of its detection in early May 2012, Flame was at the peak of its evolvement and had entered the phase of its maximum spread. By June 2012, Flame had expanded to the whole of the Middle East region. Flame was introduced into networks not in an isolated operation but rather as part of a strategy of using an extensive set of cyber tools combining spyware with programs capable of causing direct physical damage to infrastructure. It is hard to shake off the impression that Flame and Stuxnet are complementary to each other: a sophisticated instrument for gathering disparate data on any objects of interest on the one hand, and a surgically precise weapon for damaging them, on the other. The problem, however, is that accepting a purpose-driven link between Stuxnet and Flame as an axiom is impossible and counterproductive. Therefore, it is impossible to positively describe Flame as a cyber weapon.

In late May 2012 Iran reported that its oil companies had been subjected to fierce cyber attacks. The International Telecommunication Union (ITU) proposed involving the Russian company *Kaspersky Lab* in investigating this incident. The first technical reports of the incident were published on Monday, May 28, 2012. *Kaspersky Lab* specialists concluded that the attack was launched with the use of a virus of previously unseen complexity, which has become known in the virus base as *Flame*. It later transpired that the Hungarian Laboratory of Cryptography and System Security (*CrySyS)* of the Budapest University of Technology and Economics had since early May been studying a malware code that was very similar to *Flame*, if not identical to it.

How did Flame appear?

Interestingly, it is not Iran that the story of *Flame* begins with. The first versions of this malware, or rather of its prototype, were found by the American company *Webroot Community in late 2007 in Europe. The following year the virus was spotted in the UAE.* The virus had to make a long technological journey before it reached Iran in the spring of 2010 in essentially the same form that *Kaspersky Lab* specialists detected it in 2012. At the time of its detection in early May 2012, *Flame* was at the peak of its evolvement and had entered the phase of its maximum spread. By June 2012, *Flame* had expanded to the whole of the Middle East region, which makes it hard to establish the exact target its authors had intended it for. When the virus was created, it involved some advanced technologies for infecting computer systems, yet at the same time it lacked any effective mechanisms for zooming in on a specific target. Therefore the current geographical spread of *Flame* does not reflect the range or the location of its ultimate targets.

Equally unfounded is the ubiquitous use of the label “cyber weapon” in relation to *Flame*. This successor to *Stuxnet* and *Duqu* in the gallery of the world's worst cyber horrors can be described in many different ways – for instance, similar to biologists' recent discovery, as a macro virus – but the use of the term “cyber weapon” fundamentally misrepresents the essence and the purpose of this program. Those modules that have been identified and described do not have the task of disrupting computer systems, let alone of causing highly-selective, physical damage to critical infrastructure facilities, as was the case with *Stuxnet*. *Flame* is a model means of engaging in drawn-out and multilayered cyber espionage. Academic and official papers in the majority of countries with a developed IT sector usually class cyber espionage as distinct from acts of politically motivated aggression in cyberspace, hypothetical cyber wars and cyber conflicts, i.e. all those actions that can be carried out with the use of *a code-based weapon.*

Cyber weapon?

The persistent positioning of *Flame* as a cyber weapon is far from accidental - there is a hidden misrepresentation in presenting the virus from this angle. *Flame* was introduced into networks not in an isolated operation but rather as part of a strategy of using an extensive set of cyber tools combining spyware with programs capable of causing direct physical damage to infrastructure. This strategy is primarily implied to suggest actions by certain entities aimed at thwarting Iran's nuclear program. Indeed, it is hard to shake off the impression that *Flame* and *Stuxnet* are complementary to each other: a sophisticated instrument for gathering disparate data on any objects of interest on the one hand, and a surgically precise weapon for damaging them, on the other.

The problem is that accepting a purpose-driven link between Stuxnet and Flame as an axiom is impossible and counterproductive. Therefore, it is impossible to positively describe Flame as a cyber weapon. Indeed, cyber espionage by itself, despite its destructive nature, does no actual damage to the infrastructure. It would be more appropriate to compare Flame to a telescopic sight of a sniper rifle: it is very unpleasant to be caught in its sights, but it is the bullet not the scope that kills. In the case of Flame, the scope and the rifle exist seemingly separately and it is practically impossible to prove that they are used together.

In a June 1, 2012 article, *The New York Times* exposed a large-scale U.S. special operation sanctioned personally by Barack Obama, code-named *Olympic Games*, to carry out a series of attacks on Iran's nuclear infrastructure, of which *Stuxnet* was allegedly a part. While making all those sensational revelations about *Stuxnet*, the authors say practically nothing about *Flame*, although it is unlikely that the publication of such a detailed study coincided with the current hype surrounding the new supervirus by mere accident. The attempt to laconically close the topic of *Flame* with the remark that its emergence has nothing to do with the Unites States' anti-Iranian *crusade* in cyberspace, and therefore with *Stuxnet*, leaves many questions. The thing is that the NYT's key target audience – the Iranian leadership and the expert community – will not learn anything significantly new about *Stuxnet* from the article: they hardly ever doubted the U.S.-Israeli lineage of *Stuxnet* and Duqu. With *Flame,* however, things are not yet quite as obvious. Stoking up the hype around *Stuxnet* (which no longer poses an urgent threat) by making high-profile revelations about the U.S. leadership could be just an attempt to distract attention from the question of who created the new macro virus.

Furthermore, apart from captivating stories about the classified *Olympic Games* program, the *New York Times* article contains references to facts which either cannot be verified in open sources or to a certain degree run counter to known facts about *Stuxnet*. First, the authors of the article claim that in the autumn of 2010, practically right after *Stuxnet* was first detected, the virus hit 1,000-5,000 centrifuges at the enrichment facility in Natanz. However, in early December 2010 the IAEA published a report saying that some 1,000 centrifuges at that Iranian

Confidential

nuclear program facility had been shut down in late 2009 – early 2010. There were no further reports of any more centrifuges being shut down. Secondly, there are no open-source data to confirm that the centrifuges in Natanz rely on the SCADA software made by *Siemens*. This is important because the whole story with *Siemens*–made SCADA systems has been around ever since the emergence of the theory (which *The New York Times* article prefers not to mention at all) that the main target of that supervirus was Iran's first nuclear plant in Bushehr. In other words, the article in the U.S. publication, which offers valuable, albeit disputable, answers about *Stuxnet*, raises new questions about the new spying supervirus.

How does it work?

According to media reports and the expert community, *Flame* is the most complex threat to information systems to date. There are good reasons for such claims. The virus makes use of the latest achievements in malware code writing, while its size, some 20 MB of information and 70,000 lines, defies the imagination of all information security experts.

Does this quantity translate into quality? It would seem so. *Flame* uses modern techniques of infecting computer systems which were also used in *Stuxnet* and *Duqu*: vulnerabilities in autorun.inf files, in .inc files, and in the print spooler service. The use of these techniques has prompted some experts to conclude that *Flame* and the *Stuxnet* malware family were developed by the same team. Yet it is worth remembering that these are just techniques; the corresponding code is already in the public domain, so anyone can use it. In addition, the creators of *Stuxnet* used unique disguise and infection strategies: several genuine digital signatures of reputable computer manufacturers were stolen, which made it more difficult for anti-virus software to detect the virus; it also exploited a previously unused zero-day vulnerability. None of this is present in *Flame*, which uses only generally available techniques. This suggests that *Stuxnet* and *Flame* were developed by different teams but possibly commissioned by the same client.

The quality of the virus's functionality is not that great. Flame achieves its huge size primarily through the use of additional modules, which look more like a standard hacking kit rather than a high-tech virus.

Flame is capable of gathering any information from the target computer by intercepting internet traffic, collecting information about the infected system, capturing screenshots of specific processes, and recording audio and video communications. The virus has also demonstrated keen interest in the *AutoCAD* format. Yet all this functionality has already been implemented in other viruses - only this time around all of it has been collected in one place, and the assembly of various combinations of modules has been automated. This makes it possible to suggest that the supervirus may have been created by a group of *lazy hackers*, who wanted to raise their productivity through maximum automation and integration of their *business processes*. Such a simplification in the way cyber attacks are organized can lead to an avalanche-like rise in the popularity of this problem-solving method.

Earlier, a similar situation arose with DDoS attacks. For as long as the creation of botnets required considerable technological expertise and financial resources, DDos attacks were not very common. Now, however, a whole market has emerged for renting botnets at relatively cheap prices. As a result, DDoS attacks have become commonplace. A similar situation may well emerge in virus writing, when in order to achieve one's destructive aims in cyberspace, one would be able to assemble a virus from Lego-like components and modules.

Prospects for combating the virus

Irrespective of how innovative *Flame* is, the outlook for combating this new supervirus does not look promising. The main vulnerabilities are being patched; leading laboratories have started analyzing the code; copies of the virus can be commanded to self-delete from the affected systems. However, multi-module *macro viruses* increasingly look like the Rubik's Cube: the turn of one face, the installation of one new module is enough for it to continue to function using new vulnerabilities, the list of which will never be exhausted. Besides, the international practice of countering cyber threats has almost no examples of successive *preventive* action against the creation and spread of such a sophisticated virus. As a rule, top-class spyware can successfully operate and remain undetected for years. Its detection usually happens almost by accident, or at a stage when it is practically impossible to assess the total damage it has caused or to trace its origins. Moreover, in a vast majority of cases it is detected by private laboratories or national security and law-enforcement agencies that are in no way connected to international bodies. Such was the case with *Shady RAT*, *Titan Rain*, and other top-class forms of cyber spying-related illegal activities in previous years.

As a result, there is a clear *imbalance between the transnational nature of modern cyber threats and the predominantly national mechanisms of Internet security*. For the time being, the international community has in its hands not a *shield* capable of blocking the swings of an anonymous *cyber sword*, but a pair of *tweezers and some thread* to patch up the damage.

Russian approaches

> ***The direction which the efforts to rectify the situation should take is quite obvious. On the whole, it is adequately reflected in Russia's recent international legislative initiatives, including the draft Convention on International Information Security. The task is, first, to introduce the very notion of politically motivated malicious behavior in cyberspace into the political and diplomatic debate. Second, to form a truly global regime of cooperation in countering cyber threats, derived from, albeit not entirely based on, the Council of Europe's Convention on Cybercrime. The final task is to define the political, diplomatic and international legal status of cyberspace in the context of military and national security. For Moscow, the question is mainly whether it will be possible to set this process in motion before the emergence of another macro virus targeting Russian rather than Iranian networks.***

As foreign-policy initiatives are stalling, the Russian authorities have finally started to pay attention to measures aimed at ensuring the security of critical information infrastructure. In July 2012 the Russian Security Council website published what was in effect the first open document in this area: *Main areas of state policy in ensuring security of automation control systems for production and technological processes at vital infrastructure facilities in the Russian Federation*. The Russian Defense Ministry, too, is now paying increased attention to protecting critical infrastructure against cyber threats. Clearly, this cannot be attributed solely to the Middle East macro virus scares, although it appears that they have played a part, especially *Stuxnet*. Simultaneously, the Russian authorities are changing their tactics as regards the promotion of initiatives for creating a global cyberspace security regime. The Russian Foreign Ministry is now receiving assistance from Evgeny Kaspersky, whose *Kaspersky Lab* has become one of the leaders of the anti-virus industry and is confidently strengthening its positions on the world market every year. In recent months *Kaspersky Lab* was the first to detect several high-profile viruses in the Middle East, including *Flame* and *Mahdi*. It has also conducted the most detailed analysis of the *Stuxnet* and *Duqu* code. Since early 2012, Mr. Kaspersky has been actively promoting the idea of setting up a cyber-IAEA, an intergovernmental body responsible for preventing national states and affiliated actors from creating and implementing programs similar to the Middle East superviruses. Mr. Kaspersky's rhetoric is clearly in line with Russia's official initiatives and is intended to promote some of the proposals at the non-governmental level, voiced by one of the industry's most respected experts. The problem the Russian projects aim to resolve really does exist, as clearly testified by the situation with *Flame*.

Authors are research fellows at PIR Center.

Edited by Irina Mironova.

Moscow – Geneva, September 2012

Excerpts from the Membership Terms and Conditions at the Trialogue Club International

[…]

3. The rights of the Club members

3.1. Individual club members are entitled to:

3.1.3. Receive a copy of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian). According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.

[…]

3.2. Corporate Club members are entitled to:

3.2.3. Receive two copies of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian) or in both languages simultaneously. Share the bulletin with the other representatives of the corporate member. According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.

[…]

4. The duties of the Club members

4.1. All members of the Club must:

4.1.6. Not to share the Russia Confidential analytical newsletter, as well as the Password to the Club section of the PIR Center web-site with individuals and legal entities who are not members of the Club.

[…]

6. Russia Confidential

6.1. The Russia Confidential exclusive analytical newsletter is issued by the Trialogue Ltd by PIR Center's order for the Club members' private use only.

6.2. The newsletter contains exclusive analytical materials on international security, foreign and domestic policy of Russia and the CIS, prepared by the PIR Center's staff and invited experts specially for Russia Confidential.

6.3. The newsletter materials are confidential and must not be quoted and transfer to the non-members for at least 30 days since the day of issue.

6.4. 30 days after the day of issue the Trialogue Ltd can remove the exclusive and confidential status of the material, after which in such cases it is to be published in other PIR Center's editions and can be used by the Club members for quoting.

6.5. The newsletter is disseminated via e-mail between the Club members once a month in Russian or in English, depending on the choice of the Club member.

6.6. The Club member can also receive a paper copy of the newsletter in chosen language.

Trialogue

Dear Members of the Trialogue Club International,

We welcome and appreciate when the Club members recommend the Club membership and participation in the Club meetings to others. Apart from the fact that such recommendation automatically opens the door to membership in the Club, it is also ***rewarded by us in one of two ways****, which are described below. I hope that you will be interested in this offer.*

Sincerely,

Dr. Dmitry V. Polikanov
Chairman of the Trialogue Club International

Rewards for recommendation of the *Trialogue* Club International membership to others

Option 1 – Discount for membership for the next period	
5%	for 1 new individual Club member
10%	for 1 new corporate Club member
10%	for 2 new individual Club members
15%	for 3 new individual Club members
20%	for 4 or more new individual Club members
20%	for 2 new corporate Club members
30%	for 3 new corporate Club members
35%	for 4 or more new corporate Club members

Option 2 – Lump-sum compensation in cash	
100 USD	for 1 new corporate Club member
200 USD	for 2 new corporate Club members
300 USD	for 3 new corporate Club members
500 USD	For 4 or more corporate Club members