RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

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

Issue № 7 (235), vol.15. 2016

November 7, 2016

Alexey Lukatsky reports from Moscow:

ACCUSATIONS OF CYBERATTACKS: THE FACTS TO KEEP IN MIND:

Analysis of the joint statement by the U.S. Department of Homeland Security and the Office of the Director of National Intelligence accusing the Russian government of directing cyberattacks against U.S. political entities

SUMMARY

Over the past few months Russia has seen a growing tide of accusations of mounting cyberattacks against other countries. According to some U.S. politicians and media outlets, pro-Kremlin hackers are behind some of the most high-profile attacks, including the ones that targeted the Democratic Party, the WADA anti-doping agency, the U.S. national media, and election websites of several U.S. states. Even the recent leak of the NSA cyber weapons archive has been ascribed to Russian cyber criminals allegedly directed by the Kremlin. The U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (USIC) have felt compelled to make a statement officially accusing the Russian government of directing cyberattacks against U.S. political entities. Up until that moment, only China and North Korea had been "honored" in such a way.

Member of the PIR Center Advisory Board and Working Group on International Information Security and Global Internet Governance, Business Consultant on Information Security at Cisco Systems Alexey Lukatsky offers to look at American accusations and Russian reaction, show the limits and possibilities of identification the initiator of cyber-attacks, evaluate the influence of domestic political struggle and global geopolitical confrontation on the feasibility of objective investigation.

ATTACK ATTRIBUTION

According to the U.S. statement, there were two parties to the hacking incidents: the United States was the victim, and Russia was the aggressor. How accurate is such a description? When talking about weapons in the material world – i.e. nuclear warheads in their silos, military units at their bases, plane squadrons or naval fleets – it is quite clear who controls them. A naval fleet cannot be assembled by some oligarch, and no amateur can build a nuclear missile silo. The situation becomes very different, however, when talking of cyber threats. Technically speaking, the cyberattacks against the United States could have been launched from Russia, from the United States itself, or from any other country that wanted to frame Russia and to see it accused of unfriendly actions against America. All that was needed for such a frame was to lease a server at any of the numerous Russian data processing centers. Or, even simpler, the malefactor could have just hacked a computer at any of the Russian government agencies in order to make them appear the source of the attack.

To speak with certainty about who was behind the cyberattacks against the U.S. governmental and private entities, one needs to look at such attributes of the attacks as their source, their timing, and – most importantly - the attacker's motivation.

To ascertain these facts, one needs to collect concrete pieces of evidence – also referred to as indicators – that will point to the perpetrator. These attribution indicators include:

Registration of the IP address and of the domains either involved in the attack or providing the infrastructure required for the attack. These include not just the country of registration but such information as the owner of the domain or the IP address, and the owner's contact details.

Tracing of the attack to its source, or at least to the general location of the source. Many of the network devices that underpin the Internet infrastructure have the functionality required for such tracing.

Timing. Investigators often look at the time and date of the writing of the malicious code, as well as the time when the attack was launched, or when it was at its most active. With some reservations, such information can be used for further analysis. In and of itself, it cannot positively identify the perpetrator, but it can narrow down the list of countries that may have been involved in the attack.

Analysis of the malicious code itself. The code may contain comments, notes, links to websites, domain names, and IP addresses involved in the attack, as well as information about the operating system in which the code was written, the language of the code, and other regional settings.

Apart from studying fragments of the code, some researchers also try to identify the "signature" of the code-writers and determine which school of programming they come from, i.e. American, Russian, Chinese, etc.

Signature analysis is closely linked to the **linguistics** – or, more precisely, to the **stylistic analysis** of the text contained in notes, comments, references, etc. It is well-known that depending on the person's national, cultural, and

linguistic background he or she will have a different style of writing, which can be identified and pinned down to a certain geographic location.

The so-called honeypots/honeynet - this is a once-popular instrument that is now making a comeback. It boils down to creating a fake website specifically designed to attract a cyberattack, whereupon experts study the traces left by the perpetrators.

Another instrument is **classical investigation techniques** of the kind we have all read about in crime fiction. These involve undercover agents, infiltrators, supergrasses, and other sources of information that can at the very least narrow down the circle of the potential suspects.

Analysis of activity on message boards and in social networks. In some cases the perpetrator can be identified on the basis of the steps he or she takes after the attack – this is the so-called post-factum analysis. Sometimes the hackers boast about the attack or accidentally spill the beans on their social network pages. Sometimes – for example, when the target is a bank – the perpetrators can be traced by following the money. Stolen information often surfaces in the open or invitation-only online auctions and exchanges. Investigators posing as potential buyers can haggle with the seller and use the process to obtain valuable information that can help them to attribute the attack.

WHAT ARE THE PROOFS?

The joint statement by the DHS and USIC does not offer any solid proof. It contains only general phrases claiming that the methods and the motivation of the attacks point to Russia, and that the servers used in the attacks belong to a Russian company. Unfortunately, in and of itself, the address used in the attack cannot be regarded as a solid piece of evidence; it does not mean that the owner of the address was the actual perpetrator. The server may have been merely one of the numerous links in a long chain. It may have been hacked, unbeknownst to its owner. Nevertheless, the various companies that investigated the hacking of the Democratic Party's servers (ThreatConnect, CrowdStrike, Fidelis, Mandiant, and others), build their case against Russia on the one attribute – the ownership of the address used in the attack – that is the easiest to fake. In some cases they even mention the Moscow time zone as evidence of the alleged "Russian trace", forgetting that Russia is spread across nine different time zones, and that (depending on summer or winter time) Moscow itself can be in the same time zone as Turkey, Iraq, and Syria. All three countries have the potential motivation to mount a cyberattack against the United States.

The alleged evidence of the Russian government's complicity in the attacks also leaves much to be desired. For example, this is how the case against the Kremlin was put by *The Independent*: *"And who was responsible for the leak? Almost certainly, experts say, the Russians, directly or indirectly. For one thing, the Kremlin has a long record in doing this sort of thing, meddling in internal politics across Europe. Back when the DNC hack became public, in mid-June, Russian agents were identified as prime suspects".*
And this is what *CrowdStrike* had to say on the matter: *"Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with the Main Intelligence Department or GRU, Russia's premier military intelligence service".*

To summarize, Russia's accusers insist that only the Russian secret services, and no-one else, would have an interest in attacking U.S. political and military targets in cyberspace. Unfortunately, neither the IP address tracing, nor linguistic analysis, nor any other technical attributes answer the question of why the attack was launched; all they can do is try to determine the source of the attack. The only instruments that can potentially answer the question "Why?" are analysis of social network activity, post-factum analysis, and the work of agents in the field – all of which take time.

A definitive answer to the question "Why?" may be simply impossible to obtain. There are many reasons for that, including:

Geopolitics. When somebody wants to portray as certain country as enemy and construct a link between an attack and a certain government, reason and logic are often left by the wayside. Besides, identifying the real source of a complex attack routed via several countries and even several continents requires active cooperation between specialists from different jurisdictions, and from countries that may be at odds with each other.

Legal framework. Cyberspace is the only one of all the spaces (land, sea, air, and outer space) that is not regulated by any international law. All attempts at cyberspace regulation, as well as efforts to agree at least some kind of voluntary code of conduct, have failed. Another complication is that cyberspace is independent of geography. And unlike the traditional spaces in which warfare is waged, nation-states are not the only recognized actors in cyberspace. There are numerous other actors, such as armed rebels, terrorist groups, and cyber-anarchists. In essence, we are at the threshold of a new technological order, with the entire system of international law undergoing major transformations triggered by the rise of IT.

Technology. When the protocols that underpin the Internet were being designed back in the 1960s and 1970s, few must have worried about the need for positive identification of every link in the chain that takes a data packet from Point A to Point B. In fact, the entire Internet technology is based on decentralization and distributed architecture. The situation is further compounded by the lack of clear definitions; the absence of generally accepted rules or standards regarding traffic monitoring, accounting and exchange; vast volumes of traffic (resulting in short storage time for digital evidence); and the use of intermediate proxy servers.

Economic considerations. Neither the telecoms companies, nor the hosting providers or other commercial actors involved in the workings of the Internet are interested in long-term storage of digital evidence, or in conducting proper investigations of cyberattacks that would result in a clear attribution. Their priority is uninterrupted work of all their services, which requires rapid recovery and restoration of their systems to a pre-attack state, usually resulting in the destruction of evidence.

WHAT ABOUT RUSSIA?

What, then, has been Russia's response to all these charges by the U.S. media and politicians? Russia has chosen an entirely understandable tactic: don't try to explain itself, because that will be just taken as an admission of guilt. There are plenty of specialists in Russia who could conduct the attribution process and form their own opinion as to who was really behind the attacks. Unfortunately, according to Russian Foreign Minister Sergey Lavrov, when Russia asked Washington

to exchange relevant information and to let its experts have a look at the evidence allegedly proving its complicity, the United States refused. This may have been because there is no evidence – or perhaps because what evidence there is actually disproves the Americans' version that Russia was the perpetrator.

Be that as it may, Russia is currently unable to formulate its own version of what really happened.

Unlike the case of the Malaysia Airlines flight shot down over eastern Ukraine (where Russia could present evidence gathered by its own monitoring systems, as well as the results of live experiments) in the case of the cyberattacks Russia simply does not have any such evidence. Given all the aforementioned difficulties of attribution - especially if Russia is telling the truth and the attacks were staged by someone else - such evidence may be available only to the United States.

As we have demonstrated, correctly attributing a cyberattack is a difficult challenge. Also, it is perfectly clear that in the current geopolitical circumstances, certain nations can benefit from accusing other nations of staging attacks, even if those charges are not backed by any solid evidence. There are various instruments that can potentially be used to determine the source of the cyber threats, at least at the country level; these instruments aren't always used, but they are there.

Unfortunately, however, we lack the means (excepting perhaps the work of agents in the field) to differentiate between an attack initiated by a state, and an attack perpetrated by a non-state actor.

To conclude, it is worth emphasizing that correct attribution of cyber threats is a very complex challenge. Unlike the traditional threats, in the case of cyber threats we cannot identify the perpetrator or establish the motives for the attack using technical means alone. Also, special operations in cyberspace are often conducted across several jurisdictions, and their investigation requires international cooperation. That cooperation is not always possible in view of the current geopolitical climate, where some nations mistrust each other and resort to trading all kinds of wild accusations.

The author of this article is Alexey Lukatsky, Member of the PIR Center Advisory Board and Working Group on International Information Security and Global Internet Governance, Business Consultant on Information Security at Cisco Systems

Editor: Maxim Miroshnnikov

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 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 leading 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 can be published in other 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.

Dear members of the Trialogue Club International,

The 2016 Club season continues, and we are glad to **invite you to prolong your membership for 2017 or 2017-2018**, if you have not done so yet.

In 2017, the *Trialogue* Club members will continue to receive our exclusive information on the foreign policy priorities of the Russian Federation, and on current threats and challenges to global security. **Five meetings of the *Trialogue* Club International** are planned for 2017 (four in Moscow and one abroad); Club members will receive 4 issues of the Security Index quarterly journal in electronic form, **12 issues of the *Russia Confidential* exclusive analytics bulletin**, our informational and analytical newsletters.

As before, experts of the *Trialogue* Club International and of its partner organization PIR Center are open to an exchange of views on key international problems.

Fees for *Trialogue* Club membership since 2017 are as follows:

If paid **before 12 December 2017**:

Period	Individual membership	Corporate membership
01.01.17 – 31.12.17 (1 year)	45 000 rub.	72 000 rub.
01.01.17 – 31.12.18 (2 years)	81 000 rub.	126 000 rub.

If paid **before 31 January 2017:**

Period	Individual membership	Corporate membership
01.01.17 – 31.12.17 (1 год)	50 000 rub.	80 000 rub.
01.01.17 – 31.12.18 (2 года)	90 000 rub.	140 000 rub.

We would like to remind you that the corporate membership is based on **"1+1" scheme** when **two representatives** of the organization participate in the work of the Club.

On all questions concerning the *Trialogue* Club Internationsl membership, please contact us by the e-mail secretary@trialogue-club.ru or by phone: +7 (985) 764-98-96

Sincerely,

Chairman,
***Trialogue* Club International** **Dmitry Polikanov**