CHAIRE DE
CYBERDÉFENSE ET
CYBERSECURITÉ

Russian cyber activities that support strategic intelligence

Thierry Berthier (MC Univ. Limoges), Captain Djammel Metmati

January 2015, article III.19

The majority of human activities today result in the mass production of digital data. The overall volume of data produced in 2013 exceeded 4.4 zettabytes and is expected to reach 44 zettabytes in 2020. This deluge of data requires a powerful processing infrastructure and evermore powerful search engines. These allow us to collect, sort, classify and prioritize information. In the context of increasing cyberconflict, search engines facilitate obtaining data on a specific target when it has a referenced algorithmic projection.[1]

The Commonwealth of Independent States has analyzed the strategic importance of search engines in maintaining informational sovereignty, which has emerged in today's world as a powerful tool for a nation, from a technology standpoint. Hence Russia is trying to impose a national search engine on users that would limit the use of Russian data that could be used to benefit foreign powers. Added to this is their desire to control, through historic partners and alliances, architecture of information and communication systems by leveraging collaborative platforms inherent in network logic. In a crisis, this position creates vulnerabilities in the cyber architecture and sets the stage for opening access to possibly private data, and opportunities for destabilizing kinetic and cyber operations.

I-Protecting national information: the example of the Yandex search engine

In regards to the global exponential production of data, search engines are essential tools in the collection and processing of information. Each user using digital systems produces information in the form of data and metadata. Naturally, this information has become valuable in the fields of marketing and business as well as for major national security players.

With information posted online by users, operations of information warfare can be conducted even from other countries. The information offers a snapshot of the social and political context in which the data was

[1] Original phrase in French "projection algorithmique" is a concept introduced in 2013 by the author Thierry Berthier in "Projections algorithmiques et cyberespace" R2IE – revue internationale d'intelligence économique – Vol 5-2 2013 pp. 179-195.

produced. It also seems to be an important source of information for entities that oversee cyber-operations in the economic, political and military spheres.[2]

1.1. The strategic nature of search engines

Russia has measured and evaluated the impact and value both strategically and geopolitically of search engines. Created in 1997 by Arkadi Voloj, Moscow-based Yandex is the most popular search engine in Russia and the most widely used by the russophone web. The company was profitable after 2002 and was sold in 2004 for $17 million dollars. In 2012, Yandex launched its own browser "Yandex, close to Chromium in its structure,"[3] the base of which was also used by Google to develop Chrome. This browser integrates security features from a partnership forged with Kaspersky Lab. In December 2013, Yandex accounted for a total of 62% of queries and searches in Russia as compared to 27% for Google.

The Russian President recently spoke about the strategic relevance of the Russian search engine, criticizing the fact that the company Yandex is partially registered abroad. Vladimir Putin did not criticize the tax rate obtained because of this registration but instead addressed the strategic aspect and the risk of losing oversight of national infrastructure. The Russian President has publicly denounced the presence of European and American executives on the board of directors and in the management of Yandex. He said he was particularly concerned about the loss of part of Russia's sovereignty and the benefits to foreign powers. A technologically advanced nation that wishes to maintain its digital sovereignty must nurture emerging national search engines in an effort to offset the dominance of the US giants. This approach has become a priority for Russia and it can be described as a nationalist reaction.

1.1 Controlling national data

Several laws have been passed regarding internet users. They relate to the management policy of data produced by Russians. A law signed on July 4th, 2014 requires websites containing the personal data of Russian citizens to use Russian-based servers. Moreover, the law stipulates that starting on the 1st of September 2016, social networks, messaging services, search engines and user information must be hosted on Russian servers. Russian federal law[4] also requires the establishment of a blacklist of websites that contain or disseminate prohibited information in Russia.[5] It requires Russian bloggers to register their websites and to follow the same editorial rules as those in place for the Russian mass media.

This protectionist position is designed to reinforce Russia's digital power through a system that can capture and utilize data. To strengthen control in this process, the Russian state wishes to consolidate the management and processing of information going in and out of Russia to foreign territories.[6] Thus, the Russian web, locked from the inside, reflects their desire to maintain national independence.[7] Russia wants to develop a national search engine called Sputnik,[8] through which it would have more direct

[2] Especially in support of a ground, air, and maritime operations.

[3] Original quoted phrase in French "Yandex, proche dans sa structure de Chromium"

[4] Law n°89417-6

[5] Article 4 of Law No. 89417-6 envisages the creation of a register of domains and websites with pedophilia, that promote or market drugs, incite suicide or spread "extremists" ideas.

[6] Virtual and physical

[7] Other countries have taken this route. China now has a dozen effective search engines including Baidu, which surpassed Google China in popularity in 2005.

[8] The Sputnik project is supported by Rostelecom.

control than it does with the current market leader, Yandex. Information content control is approached from a national security position, from independent bloggers, to national news channels. By building cyber-architecture capable of defending the Russian network perimeter, Vladimir Putin places Russia on the offensive in relation to the "near abroad." This is illustrated by the fact that Russians harnessed the post-Cold War network architecture of Warsaw Pact countries for strategic intelligence and for use in cyber-operations. The conflict between Russia[9] and the Ukraine helps us to understand the linkage between strategic intelligence and the benefits to a cyberoperation.

According to BAE Systems, the Ukraine was the first target of particular malware[10] attacks with 32 recorded examples, and 22 examples since January of 2013. By disrupting the Ukrainian government systems with the possible capability of destroying information networks, these cyberattacks were are part of the larger conflict between the two states. Ultimately, the example shows the usefulness of cyber intelligence to disrupt the activities of an adversary state by targeting network architecture.

II- Controlling an opponent through the cyber sphere

Even with constraints, using the cyber domain appears to be an innovative way to achieve a goal at a reduced cost. The exploitation of architectural vulnerabilities in the information system of adversaries provides angles of potential attacks. They can be translated into strategic actions and creative tactics used in the management of a crisis or in actual engagement.

2.1. A cyberweapon for the heart of a network: the Snake example

The classification of this attack is based on a Trojan of the class Agent.Btz.[11] It differs from the various alternatives that have existed since 2008 because of its use of specific techniques. After installing a "backdoor"[12] on a corrupted Windows system, it provides a mechanism for communication with remote servers or machines. It then allows one to exfiltrate relevant information from a particular point in the network. At the same time, Snake is adaptable and flexible depending on the architecture of the communications system in which it operates. This feature involves precise knowledge of the mapping of the architecture of the network equipment made by the Ukrainian operator Ukrtelecom.[13] An attack was planned to take place over a week in time brackets between 10:00 and 22:00 from the 24th to 28th of February in 2014. Two peaks were recorded, one at 11:00 and the other at 17:00 and two modes of attack have been identified. The first method was executed in user mode. The second is more complex and uses a kernel infection that allows attackers to control the Windows machine. The execution of the Rootkit relies on loading a DLL module in user mode. These have various names such as taskhost.exe or service.exe, and they mask the file DLL mscpx32n.DLL. This module initiates communication with other servers in "PIPE" mode. These place this module on their white lists, allowing the infection to enter other systems despite firewalls. This operation helps to identify the internal structure of the source code.

[9] Via the Russian-speaking western Ukraine.

[10] Snake

[11] Malware affects systems running on Windows. Perceived as outdated, it remains prolific and continues to infect computers.

[12] This role is played by the different types of memory belonging to hardware manufacturers.

[13] Ukrtelecom is the only provider of landline telecommunications Ukraine.

The filenames appear and the control logs list the pseudo-developers Vlad and Gilg. These are certainly some type of malware signature. Then, a "callback" notification allows Snake to stay in the system and allows it to be able to start a new process of infection, even after it has seemingly been deleted. The Trojan remains dormant when there is no internet connection. In this case, the malicious code in the form of a DLL, is dormant in the browser. The activity of the Trojan follows that of the browser, which makes it difficult to detect. This feature is built around the nature of a webpage. The activity is a part of the different servers generating hundreds of HTTP and DNS queries. The second method of execution is quite unique. It hides in network traffic routed through an infected host and through this data is exfiltrated. However, the means of infection are traditional and include thumb drives, attachments, or vulnerabilities. Once launched, the malware is installed in a place defined as "Ultra3." The system then creates an entry in the registry with a new entry key: "KEY_LOCAL_MACHINE\System\CurrentControlSer\Services\Ultra3." The hooks[14] system masks the presence of Snake by blocking the entry of records containing the term "Ultra3." They inject the DLL in the user's environment. They adapt to the system. The injection is carried out only if the system is running "ZwshutdownSystem." If disk partitions are used, hooks such as "ObOpenObjetByname" and "IofCallDriver" hide the presence of Snake and encrypt the corrupted file. Once the connection is established with another system, the traffic is intercepted and the injection of malicious code operates several procedures connected to Windows and to the vulnerabilities of the network interfaces.[15]

2.2. Counter measures and attack stance

Immediate counter-measures are evaluated in terms of capabilities. An organization faced with these types of malware could use a "Mass scan"[16] that takes about an hour on a network where several actors are operating. By recording network flow, this method is used to track and map the path taken by the malware. In fact, the potential targets can be recognized without detection. From the machine standpoint, the use of partitions leads to the transfer of the Snake logs to this location. Also, the settings of a registry key must be changed to control the size and nature of files, and to use specific commands. The strategic and tactical consequences are on two levels.

Before a military engagement, it is possible to fire warning shots in the form of cyberattacks on the systems of adversary states. Often associated with military maneuvers, such cyberattacks seem to be part of the steps leading up to military action. Decision-makers have possible approaches structured in three stages: diplomacy, cyberattacks and military intimidation, and armed intervention. States must also virtualize their actions. In other words, sovereignty and power are also expressed in virtual networks. During conflict, interests can be protected through safeguarding virtual networks. To lose this safeguard can lead to loss of sovereignty in terms of outside access to national data and the disclosure of objectives.

While Russian cyberactions in Estonia and Georgia took the form of cyberattacks, the Ukrainian conflict highlights the ability of a state to exploit the information and communication systems of an adversary for their benefit. This approach consists of establishing one’s own network infrastructure inside the opponent's territory. Once the Trojan horse is in place, cyberoperations are facilitated by the favorable situation made possible by technology. Faced with the implications of this method, the second approach supports the organized management of data on the Russian population. Russian cyber-actions have

[14] They allow one to customize software operations according to chosen objectives.

[15] WFP is a native process that monitors the systems installed by Windows.
The network interfaces find their origin thanks to API programming interfaces. They allow the building of software, reusing features of another software.

[16] This operation allows millions of IP addresses and computer networking ports to be analyzed.

become a method for maintaining cyber and informational territory and is defended with the argument that Russian data is part of Russian strategic interests.

Chaire Cyber-Défense et Cyber-sécurité (Chair of Cyberdefense and Cybersecurity)
Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Phone number: 01-45-55-43-56 - email: contact@chaire-cyber.fr;
SIRET N° 497 802 645 000 18

The Chair thanks its partners