RUSSIAN CYBER ESPIONAGE THREATENS ESTONIAN AND WESTERN SECURITY

Russian special services continually conduct cyber espionage operations to gather information in cyberspace.

As cyber espionage is part of routine intelligence work for Russian special services, such activities do not always respond to a specific geopolitical event.

Due to the successes of cyber espionage operations conducted by the Russian special services, the Kremlin likely possesses a good understanding of Western intentions and vulnerabilities.

Russia's cyber espionage poses a major threat compared to most other countries as its special services have a long history of conducting cyber operations and are constantly exploring inventive new ways to breach information systems, develop malware and disguise their activities, while also continuing to use previously successful methods. They consistently invest resources in cyber capabilities and quickly learn from their mistakes, adapt their attack methods, replace exposed attack infrastructure, etc.

EXAMPLES OF RUSSIAN SPECIAL SERVICES' CYBER OPERATIONS THAT WERE PUBLISHED IN 2021:

- 2019-2021 Russian foreign intelligence (SVR) cyber espionage operation. SVR gained access to tens of thousands of information systems of targets through the US company SolarWinds. Other services were used in the attack. The stolen data mainly came from the US. The exact impact is still unknown.[1]
- 2017-2020 Russian military intelligence (GRU) cyber operation in France.[2]
- 2017-2021 Russian influence operations in Europe. [3]
- 2019-2021 Large-scale GRU cyber espionage operation to brute-force thousands of user passwords for Microsoft services. Both the public and private sectors were targeted.[4]
- 2021 Russian security service (FSB) cyber espionage operations in Ukraine. [5]
- 2021 Repeated SVR phishing campaigns in the West. [6]

The targets of the Russian special services, on the other hand, still lack adequate cybersecurity measures and are more likely to address their shortcomings only after being affected by a cyber operation of significant impact. To date, the targets of cyber operations have unfortunately failed to understand the need to continually maintain and invest in cybersecurity.

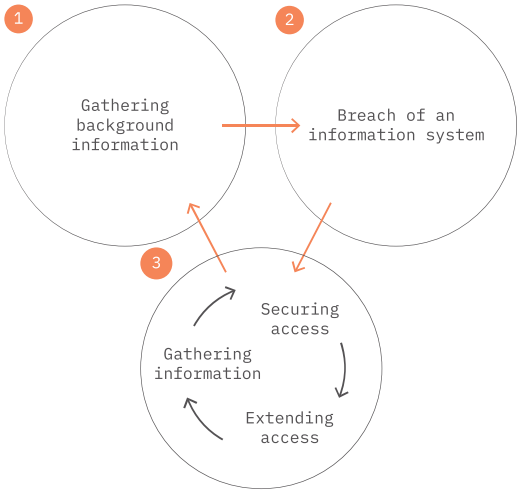
1 http://cisa.gov/uscert/ncas/alerts/aa21-116a
2 http://cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-005
3 http://consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes
4 http://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
5 http://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy
6 http://cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf

Owing to the Russian special services' activities, the Kremlin likely has a good overview of Western thinking, situational interpretations and concerns. This provides the decision-makers with suggestions on where and how to focus pressure to achieve their foreign policy goals..

STAGES OF A CYBER ESPIONAGE OPERATION CONDUCTED BY RUSSIAN SPECIAL SERVICES

A simplified description of the stages of a cyber espionage operation conducted by Russian special services follows. It is a general description of the Russian special services' cyber capabilities and does not apply to all Russian special services' centres that are capable of conducting operations in cyberspace:

Stages of Russian special services' cyber espionage operation



1. **Gathering background information**

   The special services gather background information about the target and its information systems and devices. This information is used to determine the method of attack.

2. **Breach of an information system**

   The most typical methods of breaching a target's information system include

   - phishing emails[1],
   - watering hole attacks[2],
   - exploiting security vulnerabilities,
   - using removable media[3] infected with malware.

3. **Extending and securing access and gathering information**

   Once the special services have successfully hacked into a computer network[4], they then seek to map other devices on the network. The objective is to gain the highest access rights to the entire network. After achieving this, it is almost impossible to shut the special services out of it.

   While working to extend their access rights, the special services also seek to install "backdoors" in the target's network in case they lose access through the original entry point. If the special services also lose their backup entry points to a permanent target, they will launch a new cyber operation.

   Third – and this is the primary purpose of a cyber espionage operation – they secretly gather data from the target's information system.

   Once a system has been breached by the Russian special services, there is often no remedy other than rebuilding the network from scratch.

1 Read more on these in our 2019 report
2 Read more on these in our 2020 report
3 This includes thumb drives, external hard drives and the like
4 The Russian special services act similarly when targeting an email account: they seek to secure access and collect information, including user data as well as the emails themselves. If the email account itself is of no interest, it will be used in attacks against other targets, such as sending phishing emails to the account's contacts

It is important to remember that information intended for internal use, which is not protected as strongly as state secrets, also often has high intelligence value. Holding a sufficient amount of internal information may ultimately be equivalent to having access to a state secret.

Memos marked for internal use often contain valuable information for Russia on how government agencies operate, cooperate, interpret events and make decisions.

A cyber espionage operation is largely a series of automated processes. Human involvement is limited to, for example, establishing whether the targeted person and the information on the target's devices are of interest. If not, the special services either delete their malware from the information system or use it to attack other targets of interest. In most cases, they employ various techniques to disguise their activities, such as using third-party devices to attack and gather information or breaking their malware down into components that are loaded into the targeted information systems at different times from different servers.

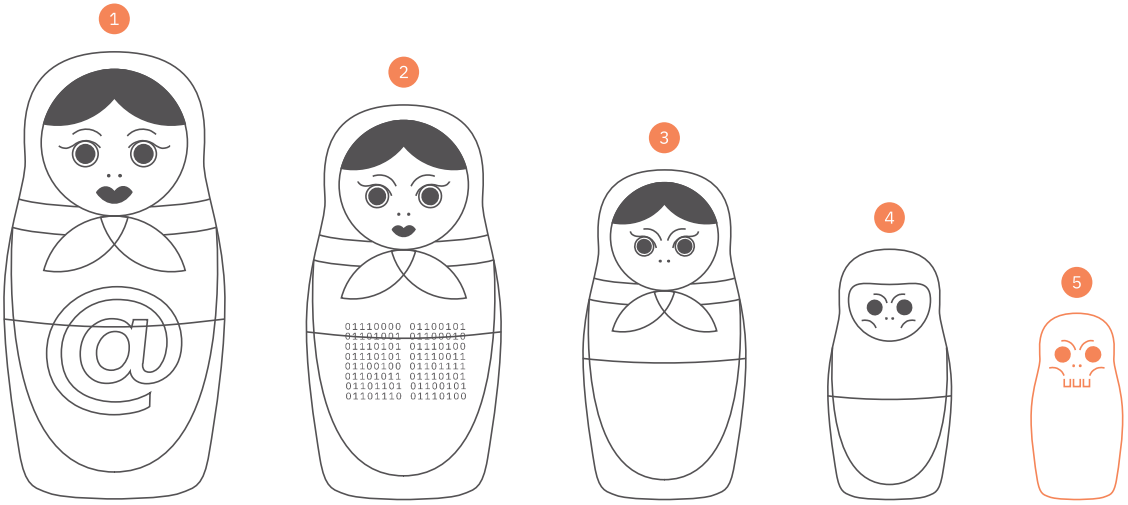
WHAT HAPPENS AFTER A BREACH?

The Russian special services use many different types of malware in their cyber operations. We will describe a method that we observed on the personal computer of a former civil servant.

The breach likely occurred when the person opened an attachment in a phishing email. The attachment only contained an initial malware component. The rest were downloaded to the computer from various locations on the internet. The malware components are like the pieces of a matryoshka doll. By opening each piece, the target launches the files inside it, which in turn transfers a new malware component performing another specific task. Once all of the malware is installed on the target's computer, regular information transfers to a server controlled by the Russian special services will begin.

In our assessment, Russian special services will continue their cyber espionage operations against Estonia and other Western countries into the foreseeable future. It is a well-established and efficient method of espionage. Therefore, the cyber threat from Russia will remain, but it can be mitigated by implementing cybersecurity measures.

How Russian special services break into a computer



1. **Phishing email**

   When clicking on the phishing email's attachment, only one part of the malware is installed on the target's computer, and other parts are downloaded from different locations on the Internet.

   At this stage, the malware checks for the existence of a cybersecurity program, and if it is detected, it will immediately stop.

   This aims to prevent cyber-savvy users from foiling the Russian special services' cyber operation.

2. **Decoy document**

   The target is then shown a decoy document to lower its vigilance and confirm that everything is in order.

3. **Creates unique ID**

   After gaining access, a unique ID is created for the computer, according to which it is possible to distinguish and identify the target. The malware also begins to transmit information from the computer to the attacker and adjusts the settings so that when the computer is restarted, the malware is also relaunched.

   The purpose of the Russian special services is to isolate infected devices and ensure access.

4. **Infects removable media**

   The malware searches for computer-connected removable media devices and network disks on a computer network, installs its software, and tries to steal information.

   How additional malware parts are loaded varies with each cyberattack.

5. **Steals information**

   Once the malware has fully installed itself on the target's devices, Russian special services will be able to regularly move information from the target's computer to a server they control and will have secured backup access.