Cyber attacks against Ukraine and possible impact in Estonia

This supplements the risk assessments sent on 25 January and 11 February – the recommendations given in both remain valid.

Situation

Cyber attacks in Ukraine continue, but compared to the ongoing Russian aggression and military activities they have been less visible and a lot less severe. There have been no massive cyber attacks on vital services or critical infrastructure, as more traditional approaches are being used to achieve primary military objectives. At the same time, various cyber attacks occur on a daily basis and play an important role in the information warfare between the conflicting parties.

The main types of attacks are Distributed Denial-of-Service (DDoS) attacks against Ukrainian (and also Russian) government websites and media outlets, but also against financial institutions and other organisations, phishing attacks, defacements (one’s own messages are displayed on a hacked website to spread them). In February, new data-wiping malware (HermeticWiper) was also found on the networks of some Ukrainian government agencies, banks and other organisations, and it’s noteworthy that the same malware was also found on the networks of the Latvian and Lithuanian branches of a company providing services to the Ukrainian government.

In addition to the activities of nation-state actors or groups closely linked to them, the ongoing war has led to a massive wave of cyber activism / hacktivism. Both the army of IT volunteers in Ukraine (mainly carrying out anti-Russian DDoS attacks) and the international hacker group Anonymous (which has claimed that it has hacked various Russian propaganda channels and acquired sensitive data of Russian government agencies) are actively working, while the ransomware group Conti has stated its support to the actions of Russia. Calls to the wider public to support Ukraine by taking part in various DDoS attacks are circulating in various social media channels.

Impact in Estonia

According to CERT-EE, the events in Ukraine pose no immediate threat to the Estonian cyberspace so far. However, this situation may change rapidly, all the more so as the risk of further escalation of the conflict remains high.

The daily monitoring carried out by CERT-EE shows that vulnerability scanning and malicious attempts to exploit them are slightly more active than usual. So far, the number of impactful incidents has not increased.

We also see the use of topics related to Ukraine and Russia as a bait:

1) in phishing e-mails trying to collect people's data;

---

11 § 12 of the Cybersecurity Act: (3) For the purpose of preventing and resolving a cyber incident, the Estonian Information System Authority sends alerts to people enabling them to take measures avoiding or reducing the impact of the cyber incident.
2) to spread malware (a malware-infected file is attached to the e-mail) 

3) in scam e-mails, where people are asked to make a donation (often in cryptocurrency) to support Ukraine (e.g. by imitating an international aid organisation).

It must also be taken into account that in addition to visible attacks, there is constant covert activity in the cyberspace – searching for access and being quietly present in compromised networks, identifying important data. It’s difficult to assess its scope in Estonia, but depending on the attacker, the motivation for such activities may be higher than usual in the context of the ongoing conflict.

The call to help Ukraine by taking part in DDoS attacks against various Russian propaganda websites was also spread on Estonian social media groups and included the suggestion to visit certain websites and enable the application (browser) on one’s device to take part in DDoS attacks against Russia. In addition to the obvious cybersecurity risks, this trend of popularising DDoS attacks could also be harmful in the long term and lead to an overall increase in Denial-of-Service attacks.

Recommendations

1. In these stressful times, every individual and every institution needs to be particularly vigilant and implement the best cyber security practices. The previous public threat and risk assessments compiled by RIA with recommendations can be found here and the public recommendations can be found here and here (in Estonian).

2. Regarding the calls to participate in DDoS attacks to help Ukraine that circulate on social media, we advise to steer clear of any such activities. The user effectively puts their device at the disposal of a botnet and runs an unknown code – both actions are unacceptable from a cybersecurity perspective.

3. When using software or applications of Russian origin (e.g. Kaspersky, Yandex), their risks must be reassessed in the current situation. One must consider that the data collected is transferred to Russia and may fall into the hands of Russian security services. Our advice is to avoid using them in both work and personal devices.

4. Users must be informed that there are currently a variety of malicious e-mails and scams circulating, using the ongoing conflict as a bait (aid to Ukrainians, NATO meeting, logistics of refugees are recent examples of themes being used). Some of these can be very credible and precisely targeted at a particular institution or organisation. Do not open any unknown files or links, and if in doubt, contact your institution’s helpdesk. Please also report such e-mails to cert@cert.ee.

The Threat & Risk Assessment was prepared by the RIA Analysis and Prevention Department in cooperation with CERT-EE.