Cyber attacks against Ukraine and possible impact in Estonia

On 13 January, a large-scale cyber attack hit the websites of the Ukrainian government. According to various sources, the websites of seventy to eighty governmental authorities, including those of the Ministry of Foreign Affairs, the Ministry of Education and Research, the Ministry of Security and Defence, and the Cabinet of Ministers, as well as the homepage of the portal for vaccination certificates, were defaced.

In addition to the defacement, there is another more serious operation: on 15 January, the Microsoft Threat Intelligence Centre announced that it had found evidence of a data-wiping malware. The malware behaves like ransomware, but it lacks a data recovery mechanism – so unlike ransomware, the goal is to erase data and render devices unusable. According to Microsoft, the malware has been found on the networks of Ukrainian governmental authorities, NGOs, and IT agencies.

How were the attacks carried out

The investigation is ongoing but according to current knowledge:

1. The Ukrainian IT company Kitsoft, which provides services to many Ukrainian governmental authorities, was compromised. A representative of Kitsoft has confirmed that they have found on their networks the destructive malware referred to by Microsoft. As the attack was carried out through a service provider, all customers of Kitsoft (including possible partners in other countries) are at risk;
2. The unpatched vulnerability CVE-2021-32648 was exploited in the CMS October content management system (the patch for this security vulnerability was released in August 2021). There are also indications that the VMware security vulnerability CVE-2021-22045 was exploited;
3. The security vulnerabilities in the Log4Shell logon feature may have been exploited. The security vulnerability of Log4Shell affects millions of devices and applications around the world, including Estonia. Read more from the blog of the Information System Authority.
4. The attackers used previously obtained accesses to the systems (leaked passwords etc)

Impact in Estonia

So far CERT-EE has not seen attacks in Estonia that can be linked to the events in Ukraine.

Nevertheless we encourage all companies and institutions to pay attention to the security of information systems, especially if the company or institution uses software products of Ukrainian origin or products that are widely used in Ukraine, or have another (IT-related) connection with Ukraine.

---

1 1 1 Section 12 of the Cybersecurity Act: (3) For the purpose of preventing and resolving a cyber incident, the Estonian Information System Authority sends people alerts enabling them to take measures avoiding or reducing the impact of the cyber incident.
Similarly to the NotPetya attack of 2017 that was carried out through updates to MeDoc accounting software, the current attack through Kitsoft service provider is a supply chain attack. Regardless of the original target, supply chain attacks tend to have spillover impact on other countries and may affect Estonia.

Recommendations for CISOs of institutions and companies in Estonia

**In the case of Ukraine-based dependencies**

1. We recommend isolating the systems communicating with Ukraine from other networks. There cannot be any outgoing connections to the internal networks from such systems.
2. The same applies to services and servers using software solutions related to Ukraine.

**General recommendations**

1. For remote work, use VPN solutions that allow multifactor authentication (MFA), all other remote services such as RDP, WINRM, SSH, etc. must not be publicly available.
2. Carry out an inventory of user accounts for remote services, including external partner access. Make sure that only necessary permissions are granted for user accounts.
3. External partners (workstations / computers / other devices) that have access to remote solutions must have security requirements in place that are consistent with the security policy of the organisation.
4. Isolate important networks and services, including public services, such as web servers. Allow only necessary inbound and outbound connections based on IP address and port. The same principle must be applied to internal traffic.
   
   **NB!** This measure is generally well implemented for inbound connections. However, in case of a vulnerable service, it is particularly important that an attacker is not able to create outbound connections to exploit the vulnerability to download malware and other tools to continue the attack.
5. Update software to the latest official version. This recommendation applies to both public services and end-user software, and also applies to software used in systems that are not directly exposed to the Internet. Make sure that the software or service is not vulnerable to Log4Shell vulnerabilities published in December.
6. Monitor logs and network traffic for any anomalies, especially remote access connections (VPN) and outbound connections of servers that are hosting public services.
7. Warn users about password phishing and oblige them to inform the information security staff if the user suspects that they have fallen victim of a phishing attack.
8. Make sure your backup solutions are up and running.
The risk assessment was prepared by: the Analysis and Prevention Department of the Information System Authority in cooperation with CERT-EE