Report to ICES partner institutes on the Cyber Attack on ICES IT infrastructure

Prepared on 29/07/2024 – Contact info@ices.dk with enquiries

Executive Summary

This report explains the key timeline and events of the cyber attack on the International Council for the Exploration of the Sea (ICES) network and infrastructure and the actions ICES took to address the attack and strengthen resilience to future incidents.

In brief, the ICES onsite servers were penetrated and we closed down our systems directly following this event. Working with specialists, the threat was identified and the entire onsite infrastructure was quarantined. The threat was removed from affected machines and the onsite infrastructure was rebuilt in a clean environment and closely monitored to ensure the integrity of the system as it was restored from clean offsite protected backups. Several steps have been taken to increase the security around the ICES systems, and additional software and monitoring have been implemented to safeguard all ICES systems, both on premises and offsite (cloud).

There has been no evidence of data exfiltration (data being copied), which has been confirmed by the cyber security specialists. Further, there is no evidence of any malware having been present in the ICES systems that could have spread to users of ICES websites, document libraries or databases. Our assessment is that the ICES infrastructure is safe and secure, although we remain at a raised state of vigilance and additional security measures are likely to be implemented over the coming weeks to further reduce future risks to our systems.

Primary Incident Details

We identified DARX ransomware on Saturday 22 June 2024 11:20 and separated our network servers Hosts that had been encrypted by a bad actor who is assumed to have used a VPN (virtual private network) vulnerability to access some of ICES onsite servers. The first activity of the malicious software was identified as having occurred on Friday 21 June in the late evening. We did not find any evidence of data being extracted or changed, nor has there been any subsequent evidence of data exfiltration. On 22 June we immediately shut down systems, VPN access, and the connection of all machines and systems to the Internet, and contacted the authorities. We identified several cyber security experts to potentially assist us, and we contracted Arctic Wolf Networks. We have examined and investigated the incident with the input and guidance of Arctic Wolf.

ICES IT team and expert cybersecurity contractors were able to rebuild and restore the systems, website, and other online resources by the week of 7 July.

Second incident: DDOS attack

On Friday evening (12 July), ICES began to experience a second attack, a distributed denial of service (DDoS) attack, which overwhelmed the web resources and led to the inaccessibility of the website and community portal (although there was no security breach of any ICES systems). From Sunday 14 July at 9 pm to Tuesday 16 July at 11:59pm, the servers received 1.19 billion hits, according to Cloudflare analysis. ICES IT team implemented solutions that brought ICES back online and enacted new monitoring protocols to prevent similar attacks.

Resolution and Remediation

ICES management and IT staff met as soon as we identified the breach, and we followed our cyber security experts' recommendations to respond to the incident. To fix the problem and resume our usual operations, we carried out the following actions:

- Performed a comprehensive scan and audit of our entire network and systems to identify and remove any traces of the attacker's activity and to ensure that no other vulnerabilities or threats were present.
- Performed a clean installation of a newer version of Windows server on all our onsite physical hosts.
- Implemented new VPN with multi-factor authentication together with Microsoft Azure Entra ID.
- Updated and patched all our software applications and installed the latest security updates and fixes.
- Changed and strengthened all our passwords for all devices and all our staff accounts.
- Encrypted and backed up all our data and stored it securely. One copy is stored in-house, and one is stored offsite on the cloud.
- Enhanced our firewall and limited the number of direct access users.
- Formatted and reinstalled the infected PCs for ICES staff and ensured all endpoints are connected to Azure cloud Entra join.
- Reviewed and revised our security policies and removed all local administrators from all accounts.
- To handle the **DDoS**, ICES has taken steps to lower the traffic of the DDoS attack. We have used anti-DOS policies, web application firewall (WAF), and temporary and targeted geo-blocking to secure the site.

Prevention and Protection

To prevent the recurrence of such an attack, we have enhanced our security and safeguarded our data and systems. We have carried out the following actions:

- We have improved and changed our antivirus software applications with ones that are even more comprehensive.
- We are updating our documentation of ICES IT systems to ensure we have accurate information on its setup and configuration.

- We have set up and activated Sentinel One protection antivirus defender with Azure Arc and turned-on live tracking and notifications of our network and systems.
- We have reviewed our implementation of regular and frequent backups and testing of our data and systems.
- We have revised our disaster recovery plan.
- Our policy is to join all user PCs only to Azure Entra ID. This way, we can track installed apps and traffic more effectively.
- ICES IT team is tracking the primary relevant and reputable cybersecurity platforms and networks to stay updated and informed of the latest threats and solutions in the cyber landscape.
- ICES implemented Cloudflare to enhance the website's security against DDoS attacks.

Data Verification and Validation

We have verified and validated our databases, documents, and applications. We have performed the following actions to verify and validate our data:

- We have compared and cross-checked our data applications with our original and backup sources and confirmed that there are no discrepancies or anomalies.
- We have used Veeam backup AI-powered malware detection functions to perform the scan on all our files/Databases before it has been restored.
- We have verified restored files/Finance systems in our internal ICES systems and have not found any trace of tampered files or data breaches.
- Our users have access to our data portal and dashboard where they can see and download our data and reports and check their validity and precision.
- Our contractor Arctic Wolf confirmed that there is no evidence or indication of any data exfiltration (i.e. theft) from ICES systems.

Next Steps

ICES continues to be vigilant and is closely monitoring all the tools we have at our disposal to ensure ICES network remains safe. We are working on further remediation measures and a 'lessons learned' analysis that will be used by ICES Secretariat, ICES Bureau and ICES Council to prioritize any additional necessary long-term changes.