NCSC
National Cyber Security Centre

2105041000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Ransomware Attack on HSE Network
2021-05-14

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	14 May 2021	CSIRT-IE	Initial Alert created regarding Ransomware attack on HSE Network

Alert

Threat Type	On 14/05/21 the Health Service Executive (HSE) were impacted by a Ransomware attack which has affected multiple services on their network. The NCSC along with the HSE and partners are currently investigating this incident and an Incident Response process is ongoing.
Details	**Background** • The Health Service Executive (HSE) has been subject to a ransomware attack likely by criminal actors. • The NCSC became aware of health sector entities detecting the human-operated 'Conti' ransomware variant on their systems during the morning of 14th of May 2021. • The HSE took the decision to shut down all of its IT systems as a precaution in order to assess and limit the impact. **Response** • The NCSC has activated its crisis response procedures and is providing support and assistance to the HSE in responding to and recovering from the incident. • The NCSC is also continuing to monitor other networks to address the risk of further attacks. The NCSC will also circulate appropriate advice following further analysis of this cyber attack. • The HSE have limited networks connectivity to other healthcare providers as a precautionary measure. **Impact** • There are serious impacts to health operations and some non-emergency procedures are being postponed as hospitals implement their business continuity plans. • The national vaccination programme is not affected.

Remediation	**Contain** 1. Isolate Domain Controllers 2. Block egress to the internet 3. Create clean VLANs for rebuild and recovery operations 4. Block malicious IPs and domain names 5. Protect Privileged accounts 6. Harden endpoints **Eradicate** 1. Wipe, rebuild and update all infected devices. 2. Ensure antivirus is up to date on all systems. 3. Make sure all hardware devices are patched and up to date. 4. Use your offsite backups to restore systems - before restoration take steps to ensure your backups have not be exposed to malware. **Recover** The 5 R's to recovery 1. Restore endpoints 2. Re-image devices if required 3. Re-set credentials 4. Re-Integrate Quarantined systems 5. Restore Services Establish monitoring of the network for further suspicious activity, particular attention should be placed on activity related to pre-cursor malware that may have pre-empted ransomware attack (IcedID/BazarLoader/Trickbot etc.).

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie