National Cyber Security Centre

2105161000-NCSC

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

NCSC Alert

Ransomware Attack on Health Sector - UPDATE
2021-05-16

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
1.1	16 May 2021	CSIRT-IE	Update regarding additional information on Analysis, IoCs and Att&ck Matrix TTPs

Alert

Threat Type	On 14/05/21 the Health Service Executive (HSE) was 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. Malicious cyber activity was also detected on the Department of Health (DoH) network early on Friday morning (14th May 2021), however due to the deployment of tools during the investigation process an attempt to execute ransomware was detected and stopped. These attacks are believed to be part of the same campaign targeting the Irish health sector
Details	**Background** • On Thursday afternoon (13/05/21), the NCSC was made aware of potential suspicious activity on the Department of Health (DoH) network and immediately launched an investigation in conjunction with the DoH and a 3rd-party security provider to determine the nature and extent of any possible threat. • Preliminary investigations indicated suspected presence of cobalt strike Beacon, which is a remote access tool. Cobalt strike is often used by malicious actors in order to move laterally within an environment prior to execution of a ransomware payload. • At approx 07:00 hrs on 14th May the NCSC was made aware of a significant incident affecting HSE systems. Initial reports indicated a human-operated 'Conti' ransomware attack that had severely disabled a number of systems and necessitated the shutdown of the majority of other HSE systems. • Early Friday morning (14th May 2021) malicious cyber activity was also detected on the DoH network , however due to a combination of anti-virus software and the deployment of tools during the investigation process an attempt to execute ransomware was detected and stopped. • 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 and Dept of Health in responding to and recovering from the incident.

Details contd.	• The NCSC is also continuing to monitor other networks to address the risk of further attacks. • The NCSC have circulated appropriate advice to constituent organisations following further analysis of this cyber attack. • The HSE have limited network 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. • For information related to HSE services, please visit HSE Cyber Attack webpage.
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.).

Analysis

The NCSC have observed a variant of Conti Ransomware and inital analysis has revealed the following:

- Cobalt Strike beacons discovered on systems suggest that it was used to move laterally within the environment prior to executing the Conti ransomware payload.
- Use of WMIC.exe to delete shadow copies:

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy
where "ID='{REDACTED}'" delete
```

- Internal network subnets are enumerated and results are saved to files
- Multiple batch files (.bat) used to copy malware to endpoints
- psexec.exe then used to execute malicious payload on endpoints using compromised user credentials
- Conti Ransomware v3 - 32 bit executable discovered
- Creates mutex: YUIOGHJKCVVBNMFGHJKTYQUWIETASKDHGZBDGSKL237782321344
- The malware will attempt to encrypt all files with the exception of the following file names:
  - CONTI_LOG.txt
  - readme.txt
  - *.FEEDC
  - *.msi
  - *.sys
  - *.lnk
  - *.dll
  - *.exe
- The malware begins by calling many bogus WinAPIs with invalid arguments to intentionally throw exceptions. These are handled by the malware and act as an anti-emulation/sandbox evasion technique
- Encrypted files are renamed with a .FEEDC extension

Indicators of Compromise

The following indicators of compromise have been observed related to this incident:

- **Conti SHA256:** d21c71a090cd6759efc1f258b4d087e82c281ce65a9d76f20a24857901e694fc
- **Cobalt Strike SHA256:** 234e4df3d9304136224f2a6c37cb6b5f6d8336c4e105afce857832015e97f27a
- **Cobalt Strike SHA256:** 1429190cf3b36dae7e439b4314fe160e435ea42c0f3e6f45f8a0a33e1e12258f
- **Cobalt Strike SHA256:** 8837868b6279df6a700b3931c31e4542a47f7476f50484bdf907450a8d8e9408
- **Cobalt Strike SHA256:** a390038e21cbf92c36987041511dcd8dcfe836ebbabee733349e0b17af9ad4eb

Indicators of Compromise contd.	• **Cobalt Strike SHA256:** d4a1cd9de04334e989418b75f64fb2cfbacaa5b650197432ca277132677308ce • **Filename:** _EXE.bat • **Filename:** _COPY.bat • **Lazagne SHA256:** 5a2e947aace9e081ecd2cfa7bc2e485528238555c7eeb6bcca560576d4750a50
Mitre ATT&CK	• EXECUTION - Windows Management Instrument [T1047] • EXECUTION - Native API [T1106] • EXECUTION - Shared Modules [T1129] • DEFENSE EVASION - Software Packing[T1027.002] • DEFENSE EVASION - Masquerading[T1036] • DEFENSE EVASION - Hidden Window[T1564.003] • DEFENSE EVASION - Virtualization/Sandbox Evasion::System Checks [T1497.001] • DISCOVERY - System Time Discovery [T1124] • DISCOVERY - File and Directory Discovery [T1083] • DISCOVERY - System Network Connections Discovery[T1049] • DISCOVERY - Process Discovery [T1057] • DISCOVERY - System Network Configuration Discovery [T1016] • DISCOVERY - System Time Discovery [T1082] • DISCOVERY - Network Share Discovery [T1135] • IMPACT - Data Encrypted for Impact [T1486] • IMPACT - Inhibit System Recovery[T1490]

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