NCSC
National Cyber Security Centre

2010301019-NCSC

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

NCSC Flash Alert

Ransomware Threat - Health Sector
2020-10-30

Status: TLP-WHITE

NCSC

Threat Type	On October 28th 2020, the United States Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) issued a joint advisory on an imminent ransomware threat to the US Healthcare and Public Health Sector. The full report, which includes Indicators of Compromise, can be found here. The report details how healthcare organisations in the United States are being targeted with Ransomware, most notably Ryuk and Conti. Although, primarily focused in the US, Ryuk has previously targeted entites across Europe. The NCSC advises organisations in the Irish Health sector to be extra vigilant in relation to this threat. **Key Report Findings:** • CISA, FBI, and HHS assess malicious cyber actors are targeting the Healthcare Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services. • These issues will be particularly challenging for organisations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.
Recommendations	The NCSC advises healthcare organisations review the IoCs in the joint advisory and take appropriate steps to scan for their existence. Some extra steps organisations can take to mitigating the threat of ransomware are: • Backups - Constituents should have an appropriate Backup Strategy. Encrypted offsite backups are critical to any recovery from Ransomware. Recovery of these backups should be tested regularly. • Access Control - Constituents should employ a policy of least permission. Only those who require access to a system should have access and the permissions that users have should be just sufficient to carry out their work. • Vulnerability Management and Patching - Deploying security patches to fix vulnerabilities in software and systems is the most effective way of preventing systems from being compromised. • User Training and Awareness Campaigns - A training programme and periodic campaigns should be utilised to raise cyber security awareness. • Implement Controls on Removable Media - Limit use of removable media, only allow access to approved users. Scan connected devices for malware. • Perimeter hardware and appliance firewalls that are positioned at the edge of the network should block unsolicited communication (from the internet) and outgoing traffic (to the internet) to the following ports: 137,138,139 & 445.