National Cyber Security Centre

2109231525-NCSC

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

# NCSC Alert

## Conti Ransomware
## 2021-09-27

**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.*

## Description

On the 22nd of September 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert in relation to the increasing number of Conti Ransomware cases that they have observed. CISA and the FBI have observed more than 400 attacks on U.S. and international organisations. The report offers valuable information on how Conti is deployed against victims. The full report can be found here.

The Irish Healthcare system was severely impacted by this same variant of ransomware this year. The NCSC recommends the following steps to help protect your organisation from ransomware:

- **Backups**
  - Organisations should have an appropriate Backup Strategy which considers how much data can be lost, commonly known as the Recovery Point Objective (RPO). All backup strategies should be subjected to periodic crisis drills whereby backups are restored to a NON-PRODUCTION environment to validate the restore procedure and the integrity of the data.
  - Encrypted offsite backups are critical to any recovery from ransomware. Recovery of these backups should be tested regularly.
  - Hardware backups is also something to be considered - do you have the right systems available to restore your data and get back to a functioning operating environment? Are the backup systems being tested and patched?
  - Immutable Backups:
    - If your organisation uses cloud storage consider the use of Immutable/WORM blobs as a backup option. Immutable storage backups are available on Azure, Google and Amazon platforms and also offer added protection in the form of PINs for user access. Immutable or Write Once Read Many storage is unchangeable once written and cannot be deleted or altered in any way. This provides an excellent mitigation against the current type of ransomware campaigns, as it stops the attacker from rendering the system unrecoverable and thereby significantly reducing their leverage in a ransom situation. Having these backups in the Cloud allows for faster recovery times in the event of a ransomware attack.
- **Access Control**
  - Constituents should employ a policy of least permission. Only those who need access to a system should have access and the permissions that users have should be just sufficient to carry out their work. Domain administrator and local administrator permissions should be restricted to System Administrators.
- **User Training and Awareness Campaigns**
  - A training program and periodic campaigns should be utilised to raise cyber security awareness.
  - Regular table top exercises should be carried out with staff to ensure familiarity with attack TTPs

- **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.
  - Vulnerability scanning should be performed regularly, and any issues patched as soon as possible.
  - Scanning of an organisations public IP ranges for systems with protocols open to the internet (e.g. RDP and SMB) should be carried out regularly.
- **Enforce Multi-Factor Authentication (MFA)**
  - Multi-Factor Authentication should be enforced on all user accounts as well as Remote Desktop Protocol (RDP) accounts.
- **Implement DMARC**
  - Implementing DMARC gives an organisation clear and measurable KPI's:
    - Know where your email comes from
    - Protect against email spoofing
    - Improve trust and simplify email processing
    - Install a Web Filter. Users clicking on links or visiting malicious sites inadvertently is still one or the major threats to network security and web filters are an extremely effective counter measure to this threat.
- **Implement Controls on Removable Media**
  - Limit use of removable media, only allow access to approved users. scan connected devices for malware
  - Prevent the use of unofficial removable media
- **Disable or Block Vulnerable Server Message Block (SMB)**
  - It is unlikely that any SMB communication originating from the internet or destined for the internet is legitimate. Disable SMBv1 and block all versions of SMB at the network boundary. Use a firewall to block SMB ports from the internet.
- **VPNs For All Users**
  - Make sure users access your network through a VPN (Full Tunnel where possible) at all times. Full-Tunnel, always-on VPNs are the preferred options as this provides all home users with access to the organization network from behind the network stack. The current climate means a significant portion of the workforce are working from home making it increasingly challenging for IT security team to ensure that networks can't be compromised via a poorly secured user device. Robust VPN services are the most effective measure to providing safe and secure remote access.

- **Have an Incident Response Plan and Playbooks Available**
  - Have a response plan ready. Consider details such as communication plans, who to notify and how.
  - Regularly test and update your response plan.
  - Contact the NCSC and notify us of the situation. The CSIRT team within the NCSC can offer assistance where appropriate and can notify the wider constituency if required. The NCSC can be contacted at certreport@decc.gov.ie or by phone at +353 1 6782333
  - Active Directory recovery should be prioritised in a recovery plan. It is important that *"In the event of a ransomware outbreak, an organisation must ensure that they have a practiced plan in place to quickly isolate key systems, and ensure that at least one Domain Controller can be quickly taken offline and safely isolated for each domain within managed and trusted forests"*[1].
- **Logging**
  - The acquisition, inspection and retention of logs are a key in the early detection of Human-Operated ransomware. Initial access via malicious email or RDP can only be detected if sufficient logging is implemented on systems. Getting a baseline of what you log and what you don't log is a good starting point. Augmentation of your current logs is strongly advised, tools such as Sysmon and Windows Logging Service will greatly enhance basic log files.
- **Disable WinRM**
  - Windows Remote Management (WinRM) is often used to spread ransomware across an organisation. WinRM should be disabled if it has been enabled on any non-server system.
- **Protect Volume Shadow Copies**
  - To hinder recovery from ransomware, shadow copies are often targeted and deleted. There are number of tools that can be deployed to prevent the deletion of Volume Shadow Copies. Constituents should consider deploying such a tool on their infrastructure to prevent such occurrences. An open source version of this type of tool is Raccine. Raccine can detect if vssadmin tries to delete shadow copies and will stop the process.

[1] https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf

**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