National Cyber Security Centre

IR-1803202001-NCSC

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

NCSC Cyber Security Advisory

COVID-19 Cyber Threat

Status: TLP-WHITE

Traffic Light Protocol

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.

1 Covid-19 Themed Cyber Attacks

The COVID-19 pandemic has caused health concerns and significant disruptions in businesses, but also created growing uncertainties among the public, health care workers, managers and policy makers. This uncertainty means people require access to the latest information and research, which creates an opportunity for cybercriminal activity.

As governments continue to announce additional measures to protect citizens by delaying the spread of COVID-19, organisations are under pressure to quickly facilitate remote working and access. The requirement to maintain business continuity may override the recommendations of IT security, and this may create opportunities for cyber threat actors to compromise IT systems. As such, it is imperative that organisations and employees remain aware of potential cyber threats they face while working within this exceptional environment.

The NCSC-IE and trusted partners have observed an increase in phishing and malware campaigns which are exploiting the COVID-19 pandemic.

Several sources have reported examples of country-specific phishing campaigns purporting to be from relevant government agencies.

Some other international agencies spoofed include: US Center for Disease Control, US State Department, and the Ministries of Health of several Asian and European countries. The World Health organisation was spoofed, and has published advice on how to detect if it is being impersonated.

Examples of Recent COVID-19 themed Cyber Activity:

- **21 February** An Advanced Persistent Threat(APT) group used emails spoofing the Ukrainian Center For Public Health to deliver a trojan, in conjunction with a disinformation campaign that triggered violent riots
- **6 March** An APT group sent emails containing a message about the outbreak from the Vietnamese Prime Minister, containing a malicious attachment
- **2 March** Coronavirus themed ransomware reported by IdRansomware team, they suggest that it acts as cover for the information stealer malware Kpot
- **13 March** Brno University Hospital in Czechia was subject to a ransomware attack that temporarily disrupted surgeries and COVID-19 testing
- **13 March** Phishing mails have been sent to workers in several international hospitals which were spoofed to be from each hospitals IT team, inviting staff to register with their user account details for a ‘Corona Virus Awareness Seminar‘
- **13 March** APT group distributed malware RoyalRoad (RAT) using decoy coranavirus themed documents
- **13 March** A Business Email Compromise cybercrime group has begun to exploit the COVID-19 event. This campaign states that they are changing their banking details in response to COVID-19 and asks for payments to new account

- **16 March** US Health Department was subject to co-ordinated DDOS and disinformation. A DDOS attack disrupted access to information on website while messages were sent with false information
- **17 March** APT group used a decoy coronavirus advisory to install Crimson RAT. This group mainly targets Indian government institutions

NCSC assesses that criminal cyber threat actors will attempt to gain access through indiscriminate phishing campaigns leading to compromised website or weaponised documents. They will exploit successful access for financial gain through blackmail, ransomware or payment redirection fraud. Invoice Redirection Fraud is often targeted and carefully researched, and may leverage the sense of urgency created by the economic damage of the pandemic.

2 Recommendations & General Advice

NCSC recommends adopting a strong defensive posture by ensuring remote services, VPNs, and multi-factor authentication solutions are fully patched and properly integrated, and by providing security awareness for employees working from home.

Organisations should review how changes in working environments may create cyber risk and mitigate according to local circumstances.

Multi-Factor Authentication: All social media, email and remote access accounts should have multi-factor authentication enabled. This is essential to protect any personal data stored on a system. If multi-factor authentication is not enabled, it is entirely possible for an attacker to 'brute force' access to an account by simply guessing a password. This remains an extremely common tactic, and enabling multi-factor authentication is the single most important step that individuals and organisations should take to protect services, personal data and infrastructure.

Password: Strength, Reuse and Sharing: Password strength is enforced by most platforms, but should be at a minimum 12 characters long. Users should consider using a passphrase to facilitate greater length and frequent password changes. Substituting certain letters in the phrase with numbers and characters will increase the security of the passphrase.

It is as important that password/passphrase reuse is avoided, including using similar passwords. Users should **take this as opportunity to change passwords for the remaining weeks of the current situation** Use of password managers such as KeePass[1] is recommended when there is a requirement on the user to remember multiple, complex passwords.
Password sharing creates significant risk to user, system and social media accounts and should not be practiced.

It may become necessary to share credential information to maintain business services. This should be done out of band, on a separate secure system environment.

Block Certain File Types:
If possible, block or monitor file types that are not normally needed for business operations (e.g. ISO files) or should not be delivered as email attachments (e.g. SCR files).

Phishing:
Phishing emails can be convincing to even seasoned IT users. A phishing email contains lure to induce the user to activate the second part, the payload. The payload contains the initial attack vector, leading to malware or sites designed to install ransomware, steal credentials or banking details, or enable further remote access to the attackers. There are some general indicators that help users detect phishing emails:

- Messages that create a sense of urgency may be trying to rush staff into making a mistake. This may leverage the economic and human damage from the pandemic

[1] https://keepass.info/

- The old rule 'If it sounds too good to be true, it probably is.' is as valid now as it ever was. Check sources, check details and context
- Grammatical errors are a red flag, official organisations will not usually send messages with simple spelling or grammatical errors
- Official organisations will usually not use personal email addresses (such as gmail.com or yahoo.com). Always hover over the sender to ensure it is who it says it is in the From field
- Hyperlinks in the email will reveal their actual destination when cursor is hovered over the link. On a smartphone, holding your finger down on a link will open details about it
- Messages that begin with "Dear Customer" or some other generic greeting require closer scrutiny, if genuine they will usually personalise their greeting

Device Exposure to malware: Devices used by workers operating outside of the organisations infrastructure may not have the same protections against malicious domains and infrastructure. This increases the risk of device compromise, and this risk may transfer to the organisations infrastructure when staff return to the workplace with the devices.
Devices should receive all security and policy updates prior to deployment for remote working. It may advisable to install additional web filtering software or make configuration changes to facilitate future infrastructure.
Before reconnecting to the organisations main network, all devices should receive security and policy updates and be subject to a full security scan.

Test Incident Response procedures: The changing workplace environment may create unforeseen issues for an organisations IT incident response. IT teams may not have access to tools or physical access to staff, devices or infrastructure. Incident response processes should be tested to identify areas that need review.
It may be necessary to provide instructions to staff on immediate actions that they should take in event of an incident, and be provided with additional contact details for IT incident response.

Protect email services Email is still the number one attack vector for cyber attacks and the COVID-19 crisis is an ideal lure for such attacks. Organisations should enhance their current email protections as much as possible. Disinformation is being spread by email impersonating credible organisations in order to sow distrust and confusion. Some suggestions, outside of the usual scanning for malicious content etc, for this might be:

- **URL Defanging** - make untrusted URLS unclickable by changing them e.g https://badsite.ie is replaced with hxxps://badsite[.]ie
- **Sender Reputation** - quarantine or reject emails from untrusted sources
- **Implement DMARC** - Email validation tool designed to detect and prevent email spoofing

As normal, incidents can be reported directly to certreport@dccae.gov.ie mailbox.

The CertReport Inbox is managed by a duty responder between 09:30 to 16:00.

This inbox is also monitored outside of normal office hours.

CSIRT-IE provides a telephone contact on +353-1-6782333.

This is monitored by the duty incident responder during office hours

3 Resources

The following are a list of sites that have articles containing specific details of COVID-19 themed attacks. These sites contain useful indicators of compromise (IOCs) and background information on the associated campaigns.

- COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/
- US Department of Homeland Security Advice https://www.cisa.gov/coronavirus
- Recorded Future - Capitalizing on the Coronavirus Panic, Threat Actors Target Victims Worldwide https://www.recordedfuture.com/coronavirus-panic-exploit
- NCSC UK Advice. https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus
- Beware of criminals pretending to be WHO https://www.who.int/about/communications/cyber-security

Feedback and Reporting

NCSC and CSIRT kindly requests any feedback users may wish to provide in relation to this advisory as regards the relevance and accuracy of the information provided. NCSC will monitor the situation Feedback can be provided by emailing info@ncsc.gov.ie or certreport@dccae.gov.ie.