Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

January - February 2024

This page is intentionally left blank

INTRODUCTION

For period 1st January- 29th February

Welcome to the latest edition of the Cyber Threat Update brought to you by the Cyber Security Centre for the Isle of Man (CSC), a part of OCSIA. This document provides an overview of cyber threats using data collected from our reporting points as well as intelligence obtained from partner agencies and open-source services.

We can only offer advice and guidance based on the information we have. Therefore, if you have any information that you believe should be considered for this document, please reach out to us at cyber@gov.im or submit it via our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Cyber Security Centre for the Isle of Man (CSC) operates a Suspicious Email Reporting Service (SERS), allowing residents to forward suspicious emails for analysis.

If you have received an email which you're not quite sure about, forward it to SERS@ocsia.im. The message might be from a company that you don't normally receive communications from or from someone that you do not know. You may just have a hunch. If you are suspicious about an email, you should report it.

Your report of a phishing email will help us to act quickly, protecting many more people from being affected. In a small number of cases, an email may not reach our service due to it already being widely recognised by spam detection services.

By sending your suspicious emails to us we can better understand the threats on our Island and provide relevant advice and warnings. Your email will also be analysed by the UK's National Cyber Security Centre (NCSC), assisting in the disruption of malicious phishing campaigns and take down of websites.

The National Cyber Security Centre (NCSC) has the power to investigate and remove scam email addresses and websites. By reporting phishing attempts you can:

- reduce the amount of scam emails you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

Since the launch of SERS, we have received over 18,312 suspicious emails. In January and February 2024, we received 1,367 suspicious emails.

SUSPICIOUS EMAILS

1,367 REPORTED

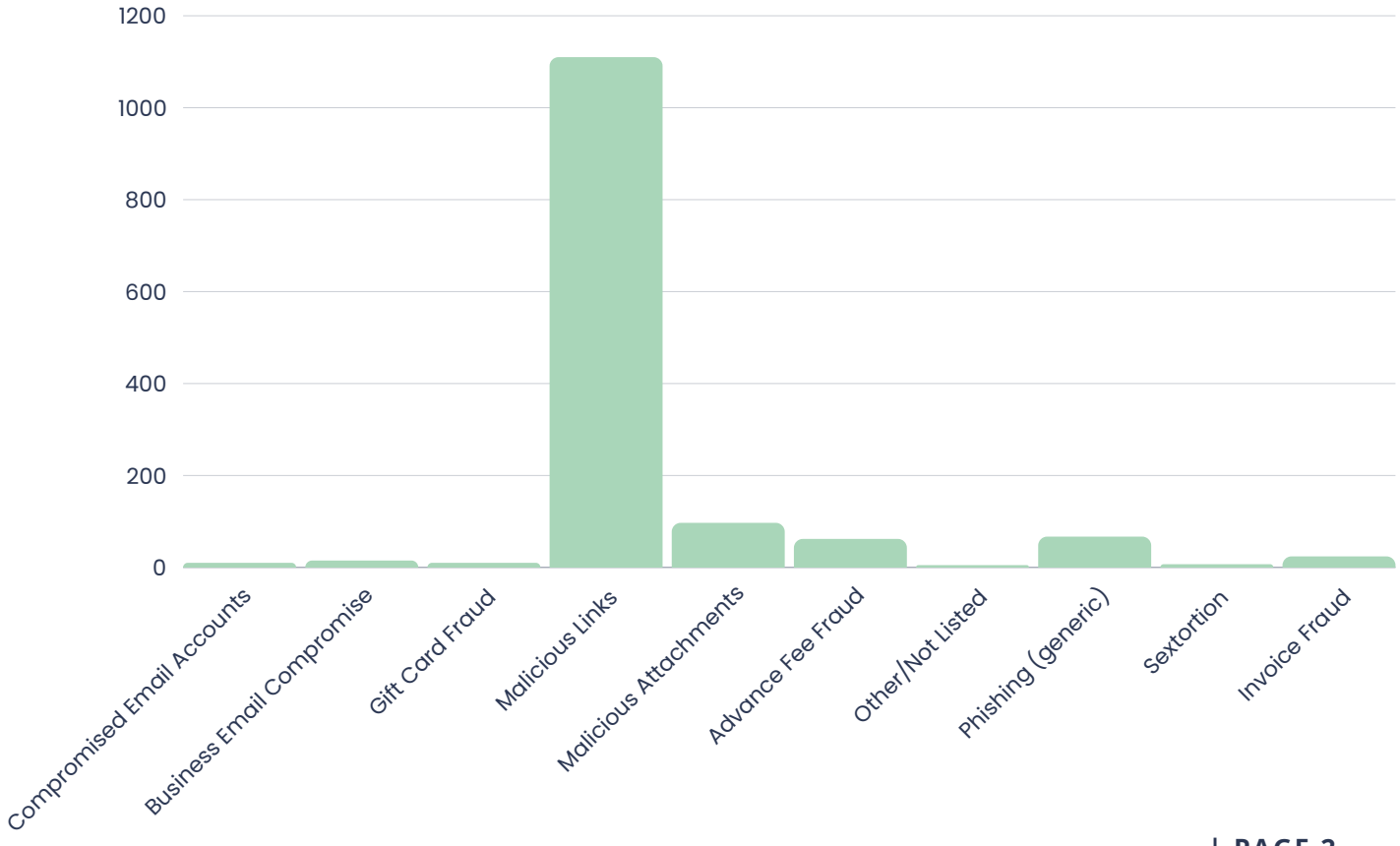
in January & February

Detail

The chart (below) details the type of emails sent by cybercriminals that have been reported to our SERS for the months of January and February. Whilst the infographic (right) showcases the top five most impersonated companies and services.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Apple
4. Retail Stores
5. Anti-virus software



CYBER CONCERNS

102 REPORTED

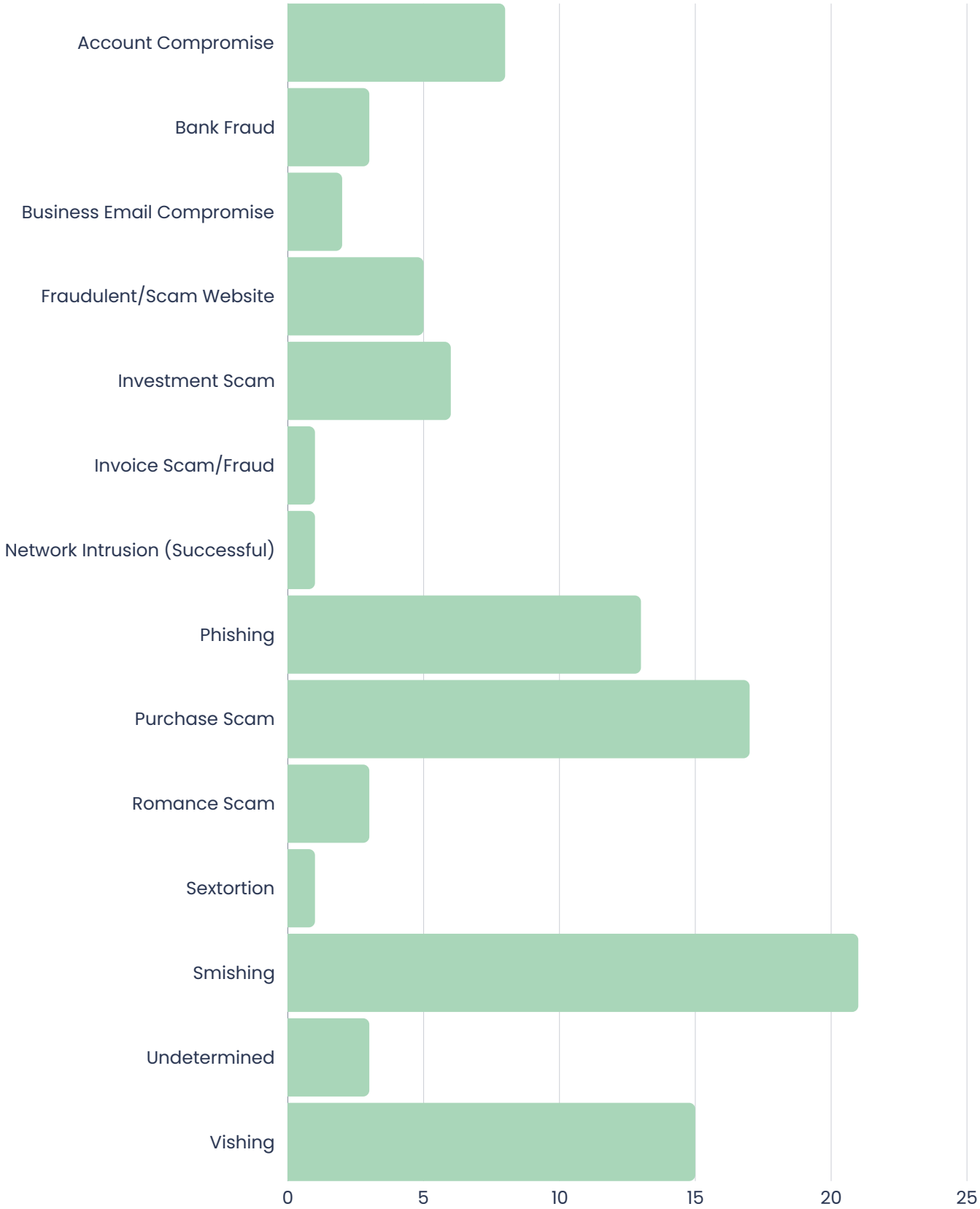
in January and February

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over January and February.

As mentioned previously, we can only provide the right advice and guidance to the public and local businesses from the information that is shared and reported to us. It is, therefore, important that we receive reports from the public and from organisations. If anyone has any information that they wish to put forward for consideration that could contribute to this document, please contact us at cyber@gov.im or report it using our online cyber concerns form.

Cyber Concerns January & February



ISLE OF MAN THREAT COMMENTARY

ACCOUNT COMPROMISE

MANX.NET EMAILS

Manx.net email scams are nothing new and have featured regularly in our reports for a number of years. The scams often come in waves with large numbers of residents hit in a short period of time, often then followed by a pause in emails before restarting again some months later.

The scams involve criminals imitating Manx.net or Manx Telecom and asking recipients to enter sensitive details to their account in order to gain unauthorised access.

However, we are also seeing the consequences of these compromises, with a large number of emails reported to our SERS showing these accounts are being used for gift card fraud with a number of victims reporting losses.

Those compromised accounts have also had rules set up by the criminal(s) to hide their malicious activity, including accessing other accounts. Furthermore, they will look at your past communications and send emails to your contacts without your knowledge. We've also seen instances where the criminals have been removed from the account but have used contacts and emails from the compromised account to continue scamming.

While falling into the period of March and not accounted for in the figures above, one high profile example included a local Parish Commissioners who had their account compromised. However, when the criminals attempted to use the compromised information, it was reported, resulting in the commissioners becoming aware of the compromise and being able to take action to recover the situation. This shows the benefits of reporting all suspicious emails and how such actions can stop the criminals.

VISHING

REVOLUT FRAUD

We received a report of a company who had received a call purportedly from the Revolut tech fraud team. The caller identified himself as Christopher Nelson and claimed there was active fraud detected on the company's mobile banking app. The caller informed the employee of unauthorised access to the mobile banking app from an unrecognised device, accompanied by multiple fraudulent transactions. To add credibility, the caller provided transaction details and sent a text message, seemingly from Revolut's official channel. This tactic significantly reduced the employee's initial concerns regarding potential fraud.

The purported Revolut representative instructed the employee to forward any login attempt emails to an email address at 'info@revolutcheck.com'. Further perpetuating the illusion of legitimacy. Subsequently, the caller initiated a series of SMS communications, apparently to facilitate the reversal of fraudulent transactions.

Initially, these transactions primarily consisted of transfers between accounts, conducted under the belief that they were part of the fraud mitigation process. However, unbeknownst to the employee, these actions facilitated the execution of the fraudulent scheme. Upon realisation of the fraudulent nature of the incident, the victim promptly initiated an internal investigation and notified relevant authorities. Additionally, measures were implemented to enhance employee awareness of social engineering tactics and reinforce security protocols when handling sensitive financial information. This incident underscores the importance of vigilance and scepticism when dealing with unsolicited communications, even if they appear to originate from trusted sources. Furthermore, it highlights the necessity of robust security measures and ongoing employee training to mitigate the risk of falling victim to social engineering attacks.

The Revolut vishing call serves as a cautionary tale for organisations regarding the potential dangers of social engineering fraud. By fostering a culture of security awareness and implementing stringent verification processes, companies can better safeguard themselves against such threats and mitigate the associated risks.

BARCLAYS FRAUD TEAM

An example seen in the period involved calls purporting to be from the Barclays Fraud Team targeting Island residents. In one instance, a client of Barclays received a call purportedly from Barclays Fraud Prevention inquiring about an unauthorised payment attempt to Argos in Glasgow. Although the client confirmed they had not initiated such a transaction, they were asked for the last four digits of their current account card and subsequently received a text message appearing to be from Barclays, further validating the legitimacy of the communication.

While away in the UK, the client received more messages from Barclays Fraud, prompting them to investigate upon their return. They discovered two attempted payments to Apple and unauthorised transfers between accounts. Contacting Barclays Fraud Prevention on a known-number immediately, they were informed that another phone had been registered to their account, suggesting manipulation by criminals. Barclays advised the client to report the incident and implemented enhanced security measures. Subsequent confirmation from Barclays revealed that the initial text message was not genuine, indicating a sophisticated smishing attempt.

Notably, the criminals operations shifted from Jersey to Isle of Man residents, with the same fraudulent transaction at 'Argos in Glasgow' being used as the hook by the scammers.

£416,771

Reported financial loses to Vishing in 2023, to find out more check out Threat Update Annual Report.

FRAUDULENT OR SCAM WEBSITES

FACEBOOK COMPETITION LINKS

While discussed in our November-December Threat report, we have continued to see a number of Facebook competition scams. In previous instances we were unaware of any victims, however, during January and February a number of victims reported their concerns to us.

Minibus Isle of Man recently conducted authentic competitions on their Facebook platform, encouraging followers to engage through comments for a chance to win. However, there have been reports of fraudulent activities associated with these contests. After commenting on the post, participants were contacted by fake Facebook pages, falsely claiming they had won and directing them to malicious phishing websites aimed at extracting sensitive information.

It's important to note that these fake pages can be distinguished from the genuine ones through various indicators, such as the absence of an 'author' tag on posts and significantly lower follower counts, post frequency, and creation dates compared to legitimate pages.

Comment from scammer directing respondent to phishing site

PHISHING

FACEBOOK DRIVING LICENCES

Media coverage and reports received to us highlighted multiple Facebook pages offering Isle of Man driving licenses without a test. The pages offering services that were obviously not legitimate were reported to Facebook who took no action.

Whilst an obvious scam and usually not worthy of being featured, the pages generated enquiries about the use of peoples personal information that was displayed on pictures of the driving licences.

Upon investigation we found that, whilst some of the images were templates taken from the Isle of Man Government Website, other images with personally identifiable information had been posted on Facebook. These posts were from residents who had found lost driving licences and wish to return them to their owners.

Whilst posted in good intentions, we wish to highlight how important it is to not post official documents onto online public forums. Once these images are posted the details can be scraped and victims lose all control of the information scraped.

Scam post using photo obtained from Facebook

ROMANCE FRAUD

An elderly resident was contacted through Facebook and formed a companionship with an individual whom she believed to be her romantic partner. The persona portrayed on Facebook depicted a prosperous Canadian Actor of 49 years of age. Over a period of approximately four months, they maintained daily communication. Subsequently, the individual on Facebook requested a sum of £3,000 purportedly to cover veterinary expenses, which the Isle of Man resident promptly transferred. The request stipulated that the payment be directed to an assistant (of a different name) due to the absence of a personal account.

Later that day, the Isle of Man resident received a phone call from an individual claiming to represent the fraud department, asserting that the initial payment had been intercepted. Under threats of legal consequences, the criminal coerced the Isle of Man resident into transferring an additional £12,500 to investigate the disappearance of the initial £3,000. The caller, exhibiting a Scottish accent, conveyed a sense of surveillance over her activities.

Following this, two days later, the same Scottish individual made another demand for £50,000 under the guise of directing it to the Isle of Man, instructing the Isle of Man resident to inform the bank that the transfer was intended to settle a relative's mortgage. Despite an attempt to comply, the bank intervened and halted the transaction due to conflicting information provided by the Isle of Man resident.
In response to these events, the Isle of Man Bank's fraud management team is actively pursuing the retrieval of the £12,500 and has implemented precautionary measures to safeguard the victim’s bank account.

This incident highlights the risks of romance scams and the need for caution when interacting with strangers on social media. It's crucial to verify the identity of individuals before sending money. Be wary of coercion tactics and threats, and report any suspicious behaviour promptly. Banks play a vital role in detecting and preventing fraud, but individuals must also prioritise digital literacy to protect themselves from romance fraud.

EXTERNAL THREAT COMMENTARY

LOCKBIT – LATEST ATTACK ON FULTON COUNTY GEORGIA CLAIMED

The ransomware group known as Lockbit has claimed the cyber-attack on Fulton County, Georgia as their own and are threatening to publish confidential documents if the ransom demand is not paid. The attack, which occurred in the last week of January, was confirmed by a Fulton County spokesperson following the release of 25 screenshots by Lockbit, proving that they had gained access to the County's systems and stolen confidential information.

The attack has impacted many of the County's key services. Phone lines went down, however, one out of three affected phones were restored. As of February 14th the property tax system is still offline, with payment processing and other transactions are still unavailable. Citizens are unable to pay their water bills electronically, however, late penalties have been wavered as a result of the attack. There have also been delays in the justice system, but their email services have remained unaffected. Priority in the recovery process has been given to election offices ahead of early voting opening at the end of the month ahead of the March election.

By the end of the period, Fulton County had not paid the ransom demand, letting the payment deadline pass without consequence. Screenshots of the data leaked by Lockbit were removed from their website after the February 16th deadline passed, suggesting that the group had moved onto another victim after realising that Fulton County would not be paying the demand.

INTERNATIONAL LAW ENFORCEMENT COALITION TEMPORARILY DISMANTLES LOCKBIT RANSOMWARE GROUP, CHARGES FIVE RUSSIAN NATIONALS

Following on from the Fulton County attack, a massive international law enforcement operation has successfully disrupted the notorious cyber-crime gang Lockbit, leading to charges against five Russian nationals involved in the group's operations. The US authorities have taken legal action against the individuals, with two already in custody, Mikhail Vasiliev in Canada awaiting extradition and Ruslan Magomedovich Astamirov detained in the US. However, three others: Artur Sungatov, Ivan Kondratyev, and Mikhail Pavlovich Matveev, remain at large.

Named 'Operation Cronos', coordinated by the UK's National Crime Agency (NCA), the FBI, Europol, and a coalition of international police agencies, resulted in the seizure of Lockbit's command and control infrastructure. Additionally, more than 200 cryptocurrency accounts linked to the criminal organisation have been frozen, disrupting their financial activities.

Lockbit, known for its ‘Ransomware-as-a-Service’ model, has been responsible for numerous cyber-attacks globally, targeting businesses and individuals. The group's primary administration environment, responsible for managing and deploying hacking technology, has been seized by law enforcement.

Graeme Biggar, the NCA's director general, emphasised the significant disruption caused to Lockbit, stating that the operation has damaged the group's capability and credibility. Furthermore, the campaign recovered over 1,000 decryption keys intended for victims, aiding in the recovery of encrypted data.

Unfortunately, as expected, Lockbit was not setback for long. In under a week the ransomware operation was relaunched on a new infrastructure, with threats made to focus attacks more towards the government sector, in retaliation to action taken by law enforcement. The involvement of Russian hackers in cyber-crime has been a challenge for law enforcement agencies, but this operation marks a significant milestone in combating such threats. The collaborative effort demonstrates the determination of international authorities to tackle cyber-crime, and provides a warning to cybercriminals that they are not invincible to law enforcement.

BLACK BASTA RANSOMWARE GROUP: SOUTHERN WATER CYBERATTACK

Southern Water, headquartered in Worthing, West Sussex, has issued an apology after confirming a cyberattack that resulted in stolen personal data from some customers. The firm reassures customers that water supply remains unaffected. An investigation launched on January 22 revealed a cyber-criminal organisation's claim of stealing data from Southern Water's IT systems.

Between five and ten percent of customers' details were stolen, in addition to an undisclosed number of current and former staff. The Black Basta ransomware group claimed responsibility for the intrusion, though Southern Water hasn't confirmed ransomware involvement. Names, dates of birth, national insurance numbers, bank account details, and more were exposed online.

Affected individuals will receive letters and a free 12-month Experian Identity Plus membership for credit monitoring. The utility company serves millions of customers, potentially impacting hundreds of thousands.

Southern Water has been collaborating with government, regulators, and cyber-security authorities, including the National Cyber Security Centre. Enhanced monitoring and protection tools are deployed to prevent further breaches.

While Black Basta removed its post about Southern Water, indicating a possible ransom payment, the utility company declined to comment. The incident underscores the vulnerability of critical infrastructure to cyber-threats.

ROMANIA – LARGESCALE RANSOMWARE ATTACK TAKES DOWN HOSPITALS

The Romanian Ministry for Health have confirmed that systems are down due to a ransomware attack that began on February 11th. The ransomware targeted the Hipocrate Information System (HIS) healthcare management system, which became non-functional. Once the system was down hospital staff were unable to access files and databases and this forced patients to wait in emergency rooms as their health records could not be accessed.

It was initially estimated that 15-20 hospitals were experiencing problems with computer systems, however, this number is now estimated to be over 100 that have been affected in some way. The affected facilities include specialist, children's and emergency hospitals. The actor behind the attack is still unknown, as the ransom note provided only included an email address and a demand of 3.5 Bitcoin (over £130,000).

The attack is believed to have been started through a flood-type cyber-attack towards a certain class of hospital IP addresses, originating from a botnet network. While the attack is analysed and a solution is trying to be developed the hospitals have resorted back to paper medical notes and charts, public internet access has been stopped, and the systems are working offline.

Staff at the affected hospitals have been recommended not make contact with the ransomware group through the provided email and to not pay the ransom demand to try get vital files decrypted. According to Romanian cyber officials, the impact of the attack has been reduced as hospital data had recently been backed up, highlighting the importance for critical infrastructure to make sure they are regularly backing up their important data.

IRAN AND NORTH KOREA – CAUGHT USING AI IN HACKING ATTEMPTS

On February 14th it was revealed that Iran and North Korea, and to a lesser extent Russia and China, have begun using generative-AI to organise and carry out offensive cyber operations. Microsoft, along with collaborative partner OpenAI, have detected that these nations are actively using or attempting to exploit AI technologies they have developed.

Since the launch of ChatGPT in November 2022, concerns have been growing surrounding the potential weaponisation of advanced AI tools by adversaries. Chinese state-backed hackers are experimenting with the use of Large Language Models (LLMs) to ask questions about rival intelligence agencies and notable individuals. North Korea are using generative-AI and LLMs to generate content that can be used in spear-phishing campaigns, while Iranian hackers are using them to generate more convincing phishing emails.

While current use of AI in hacking attempts is in the early stage and 'incremental', it is important to highlight that large cyber threat organisations are beginning to try and enhance their attacks through the implementation of AI and LLMs.

Following on from the discovery, Microsoft and OpenAI have rolled out a blanket ban against state-backed hacking groups from using their AI products, as they do not wish to facilitate threat actors perpetrating campaigns against anyone.

CYBER GLOSSARY

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

Common Vulnerabilities and Exposures (CVE): The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation - GDPR: The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on 25th May 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

Phishing: Phishing is a type of fraud in which the attacker attempts to steal sensitive data such as passwords or credit card numbers, via social engineering.

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

Vulnerability: A vulnerability is a weakness that allows an attacker to compromise security (integrity, confidentiality or availability).

CLICK HERE OR SCAN TO VIEW OUR FULL CYBER GLOSSARY

ABOUT US

The Cyber Security Centre for the Isle of Man (CSC) was launched as a branch of the Office of Cyber Security and Information Assurance (OCSIA) in October 2023, to increase our presence in the public sphere. The CSC is responsible for providing targeted advice and guidance to individuals and businesses, while OCSIA remains for Information Assurance within Government.

Our objective is to improve cyber resilience of everyone who lives or operates in the Isle of Man. Our commitment to supporting individuals, businesses and the private sector is at the heart of what we do, and we are devoted to maintaining partnerships with everyone who needs us, while raising awareness about the rapidly changing cybersecurity threat landscape.

Established in 2019, our annual one-day cybersecurity conference ‘CYBERISLE’ takes place in autumn, and acts as a focal point event in the field on Island. We bring together leading experts, students, charities and individuals, to share ideas and allow everyone to gain a deeper understanding of current cyber threats to our Island, and the best mitigation tactics available for increasing nationwide cyber resilience.

CYBERISLE 2024

After the success of CYBERISLE 2023 we've began the early stages of planning the next instalment of the Islands premier cyber security conference. Keep an eye on our website and social media using the links below.

@CyberIOM

facebook.com/OCSIAIOM

linkedin.com/company/csc-isle-of-man/

Join our mailing list

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

CSC Cyber Security Centre for the Isle of Man

a part of the Office of Cyber-Security & Information Assurance

csc.gov.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin