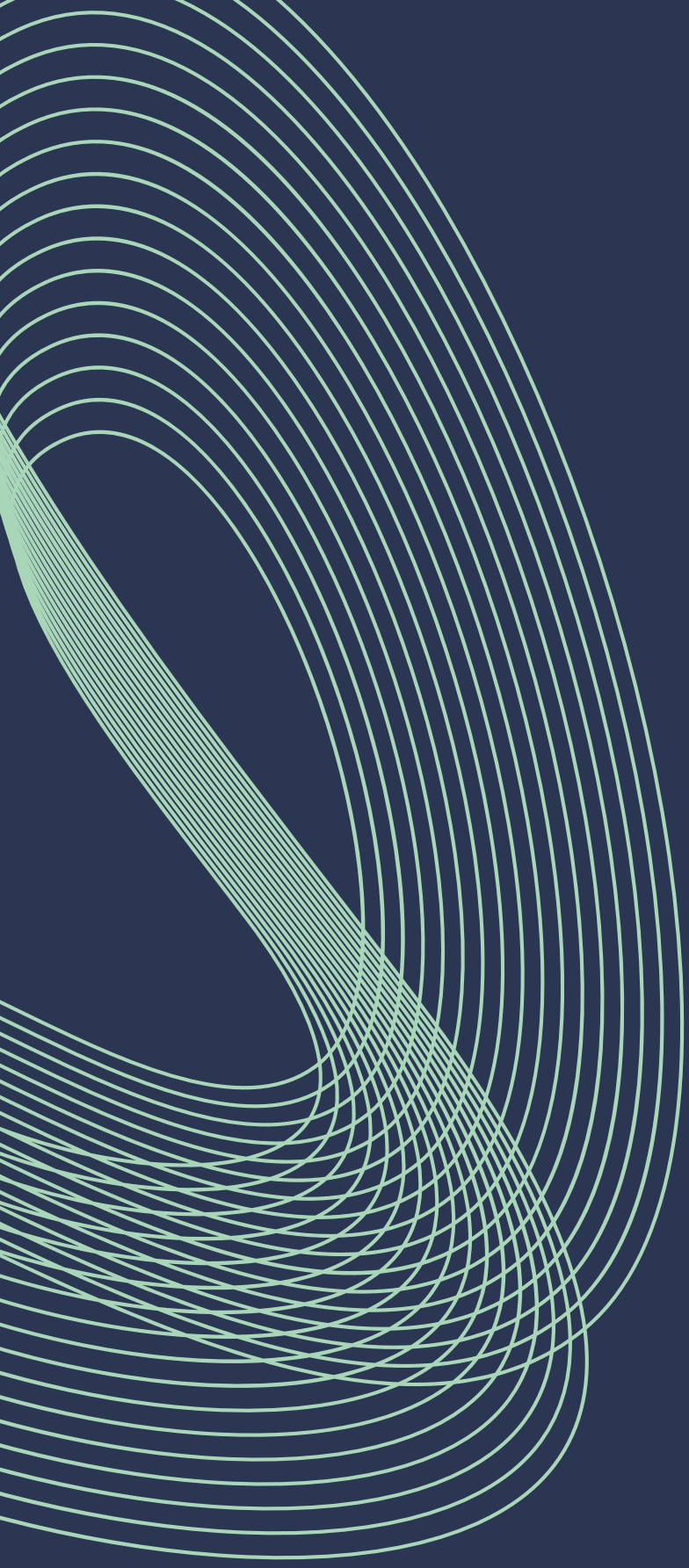
Cyber Security Centre for the Isle of Man

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

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

March - April 2023



INTRODUCTION

For period 1st March- 30th April

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 sharing with the private sector.

If anyone has any information they wish to put forward to be considered for this document, please contact the CSC on cyber@gov.im or report it using our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Office of Cyber-Security & Information Assurance (OCSIA) introduced the Suspicious Email Reporting Service (SERS) an automated system used to gather intelligence and take down malicious URLs on 23 October 2020.

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) 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 11,800 suspicious emails. In March and April 2023 we received 987 suspicious emails.

SUSPICIOUS EMAILS

987 REPORTED

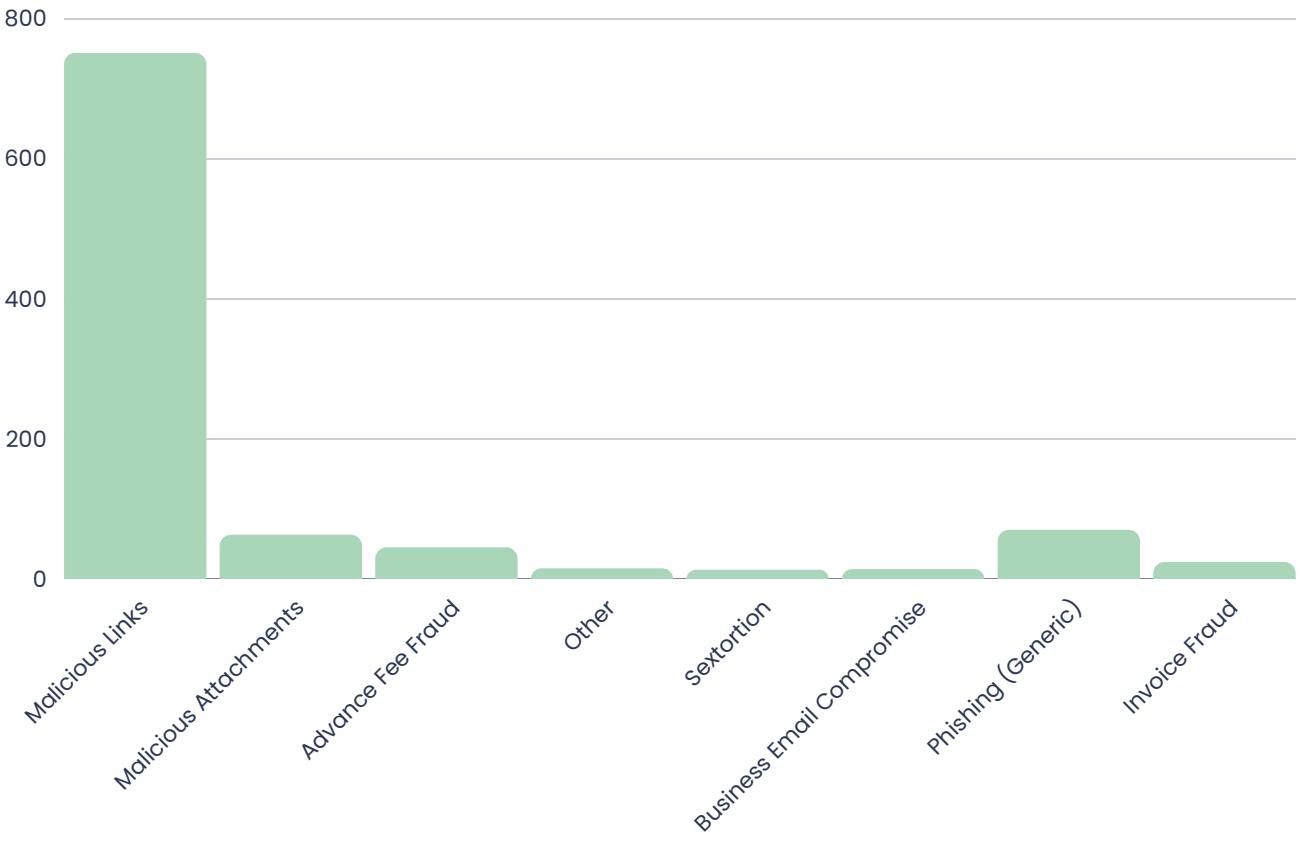
in March & April

Detail

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

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Romance/Dating/Sex
3. Parcel Delivery
4. Pharmaceuticals
5. Antimalware Software



CYBER CONCERNS

73 REPORTED

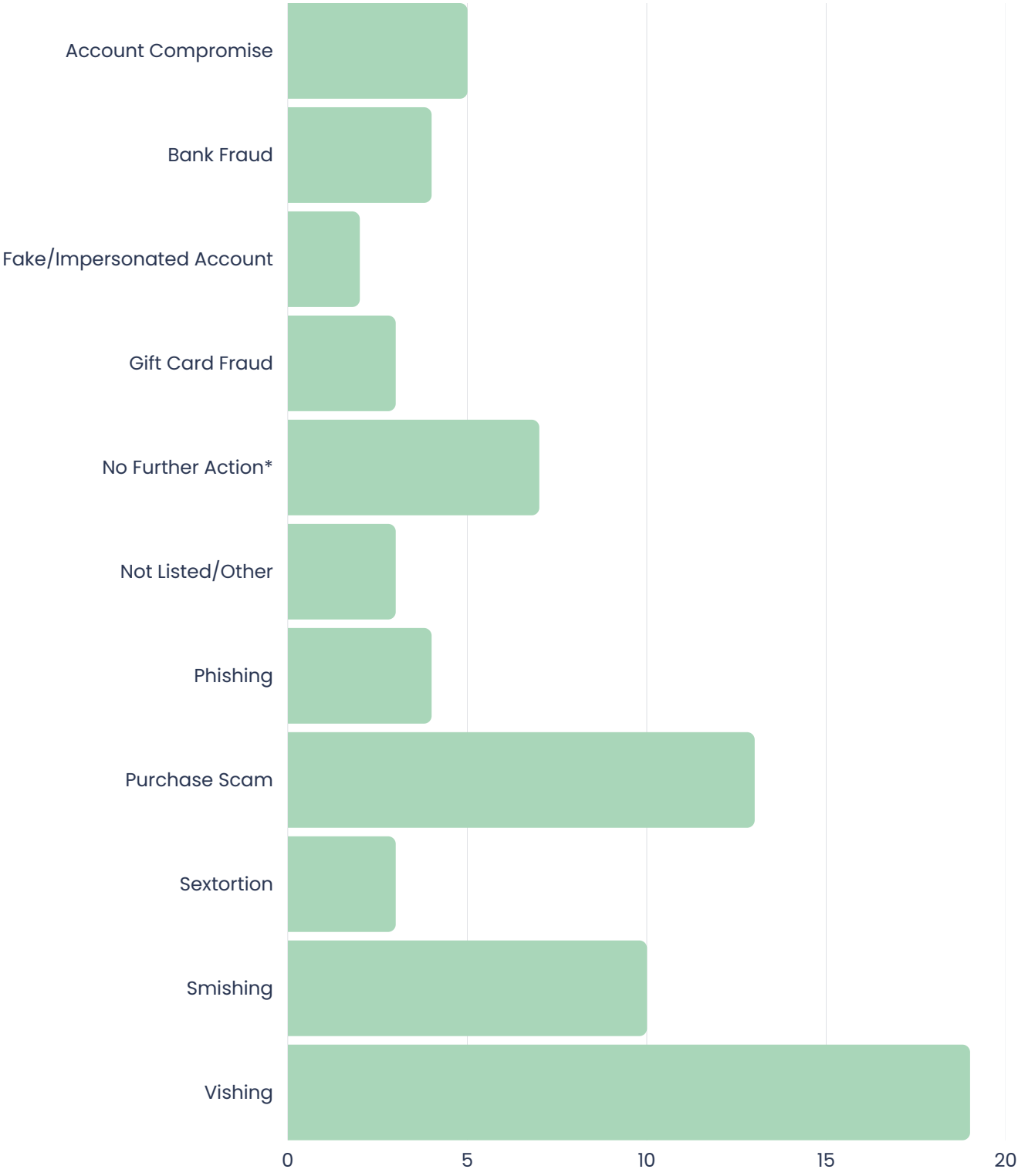
in March and April

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over March and April. This month has seen a small decline in the number of reports; this reflects what we are seeing anecdotally with the majority of scams coming in the form of Facebook-based purchase scam, which we know appear and disappear equally as fast.

One other possible reason for this is the crackdown on cyber crime by agencies such Europol, with 288 dark web vendors arrested last month and the disruption of an online investment scam being notable highlights. Whilst speculative, there could be correlation between criminals wishing to keep a low profile and the decline in reports that we've seen over the past two months.

Cyber Concerns March & April



***No Further Action:** submitted with good intentions but after further investigation was found to be a non-cyber concern or communication was found to be legitimate.

ISLE OF MAN THREAT COMMENTARY

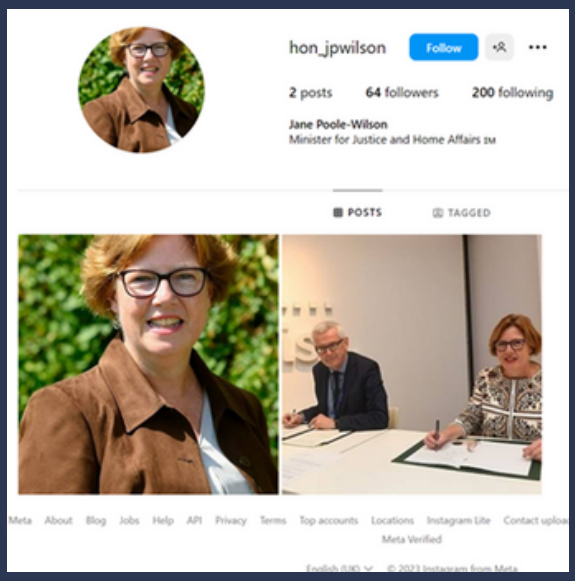
In order to gain a more detailed understanding of the types of incidents that are contributing to trends, this section presents case studies of specific threats outlined on pages 3 and 4. These case studies, all taken from our cyber concerns reporting tool, provide insight into the methods and motivations of attackers, as well as the impact that these attacks have had on the affected parties.

FAKE/IMPERSONATED ACCOUNT OR PROFILE

MHK INSTAGRAM ACCOUNTS

In March, we were alerted to an Instagram account impersonating Minister for Justice and Home Affairs, Jane Poole-Wilson. Whilst initially unclear of the fake accounts objective, it was subsequently discovered that the account was used to defraud victims through investment scams. The account used publicly-available photography of the Minister to add legitimacy.

OCSIA took steps to support the Minister to have the account removed, however, this incident demonstrates the relative ease of impersonating people on social media, with Instagram making the process even more difficult for those who are not already on the platform. We have subsequently been made aware of other 'fake' accounts involving other Tynwald Members and we are working with departments to have these taken down.



PURCHASE SCAMS

This month has seen purchase scams becoming the second-most reported cyber concern, and one that has seen substantial amounts of money taken from victims. The primary platform used by criminals is Facebook; the website's reliance on groups to self-moderate means scams are often not taken down before someone becomes a victim.

These scams rely on some users of Facebook having to trust that the profile they are communicating with is genuine. Often this trust can be based on having seen a name and face that seems 'real'. However, these names are made up and images are taken from the internet. At OCSIA, part of our job involves helping members of the public to understand that the levels of trust you apply to real life should not extend to the internet.

These scams are often performed one of two ways. One option is the scammer makes a new profile with a fake name and images taken from the internet. For anyone prepared to look, the profile can be identified as fake. The more convincing method involves a compromised account of a legitimate person, where the scammer uses already-established relationships to scam victims out of money. In the period we saw this occur with a well-known local figure whose account was hacked and used to sell non-existent puppies.

A list of all purchase scams on Facebook that were reported are given below. What is interesting to note is that all but one victim (or potential victim) were people selling an item rather than making a purchase.

14 March – Loss of £49.49 – Clothing sale
20 March – Loss of £320 approx. – iPhone sale
4 April – Loss of £50 avoided – Clothing sale
4 April – Loss of £950 – unspecified item
17 April – Loss of £1,000 avoided – Rental deposit

GIFT CARD FRAUD (AGAIN)

Gift card fraud continues to be problem owing to the unique characteristics of these cards: the transfer of funds from a gift card cannot be remediated and scammers often use the funds immediately after the receipt of codes. These offer advantages to scammers over other types of transactions.

In this month's reported cases, a scammer, pretending to be a friend, contacted someone using Facebook Messenger and gave details of a claim that could be made that would lead to a reward of £30,000 from a grant fund. More messages were then received from an unknown Facebook profile who claimed to be an Agent for the fund. This Agent encouraged the purchase of multiple gift cards and then requested the unique codes on those cards. The victim in this case lost £2,100 and realised they had been scammed when a further £1,500 was requested.

Whilst gift card fraud is commonly-associated with business emails (which then transition to WhatsApp), we are noticing a trend of scammers diversifying their targeting methods and taking advantage of the previously-mentioned levels of inherent trust Facebook profiles provide.

CLICK HERE OR SCAN TO SEE OUR ADVICE ON GIFT CARD FRAUD.

WHY REPORT INCIDENTS?

As one of our sources of threat intelligence, our Cyber Concerns reporting form provides us with up-to-date intelligence on the latest threats and scams reaching the Island. For us to keep you informed and keep you safe, it is important that we see as many of the scams and frauds that are happening on the Island, but we can only do this if you tell us about them. These reported concerns not only feed into this document but are also disseminated to our network of private-sector partners so they can take appropriate action.

By acquiring a large number of reports, we are better able to evaluate the data and pass on key messages. With more reports, we are better able to see if a cybercrime is a one-off or part of a larger campaign affecting residents and organisations across the Isle of Man. We don't just create advisories and warning messages: wherever possible and necessary, we will provide confidential advice and guidance to minimise any loss or harm to the Reporter. In some cases, particularly where we see a criminal campaign, we will liaise with partner agencies and local entities to implement technical controls to minimise future risks and victims.

Where a crime has been committed, your report is logged (and feeds into intelligence) and the police are then informed, who will then take over the case. Where account details are identified, we work with our partners in the Financial Intelligence Unit (FIU) who coordinate with banks to have criminal accounts shut down.

All reports are kept in the strictest confidence, and details are only disclosed with the consent of the reporting party.

EXTERNAL THREAT COMMENTARY

OPENAI CHATGPT – REDIS BUG – DATA BREACH

ChatGPT is an AI chatbot that uses human-like conversational dialogue to respond to questions and compose various written content such as articles, social media posts, essays and code. It is similar to automated chat services found on websites when users need help.

ChatGPT works by using specialised algorithms to find patterns within data sequences. It uses GTP-3 language model, a neural network machine learning model and a third-generation of generative pre-trained transformer that pulls a lot of data to give the response.

A bug in the Redis open- source library was behind a recent exposure incident of ChatGPT Users' data. Some subscription confirmation emails that were generated during the time were sent to wrong users because of this bug. The company explained that just hours before the disruption it was possible for users to see another user's name, email address, the last four digits of the credit card number and the credit card expiration date.

The Redis Bug originated in the redis-py library and was responsible for exposing users' personal information and chat titles. This happened from corrupted connections that returned unexpected data from the database cache making information belonging to other users available to see.

3CX DESKTOP APP – LABYRINTH COLLIMA – CYBER ATTACK

A hacking group, known as Labyrinth Collima, and believed to be backed by North Korea, is suspected to have compromised the 3CX desktop app in a major supply-chain attack.

3CX is a software-development company whose phone-system software is used by over 600,000 companies. Companies who use 3CX software include multinationals such as McDonalds, BMW, IKEA, and Coca-Cola and another user is the UK's National Health Service. The 3CX desktop client software allows businesses to make and receives phone calls over the internet using Voice-over-Internet Protocol (VoIP) technology.

The targets of these attackers consist of both Windows and macOS users with the compromised 3CX softphone app. In order to achieve this attack it appears they used digitally-signed and trojanised version of the software to target both Windows and MacOS 3CX customers.

The malicious activity that has been identified includes beaconing, which is the sending of signals to infrastructure controlled by the attackers, installing additional software, and directly manipulating a targeted computer through hands-on keyboard activity.

One of the most common post-exploitation activities that have been observed is the creation of an interactive command shell, which is a tool that attackers can use to give direct and remote commands to a computer.

The attacks appear to have begun on 22 March 2023; the extent of the attacks is currently unknown.

3CX customers are encouraged to visit the Company's website for the latest software updates, https://www.3cx.com/blog/news/desktopapp-security-alert-updates.

TAIWANESE PC VENDOR MSI – MONEY MESSAGE RANSOMWARE – RANSOMWARE

MSI (Micro-Star International) is a hardware giant known globally for making motherboards, graphic cards, desktops, laptops, servers, industrial systems, PC peripherals and infotainment products.

MSI suffered a data breach following a ransomware attack. Money Message demanded a $4,000,000 ransom on claims they had stolen 1.5TbB worth of documents from MSI and threatened to leak the data online if the company refused to pay the ransom. Even though there was a breach, MSI reported there has been no significant operational or financial impact as they have security enhancements implemented to ensure that the data stored on the affected systems are secure.

Money Message listed MSI on its data leak website posting screenshots of what they claim to be MSI's CTMS (Central Trail Management System) and ERP (Enterprise resource planning) databases and files containing software code, private keys and BIOS (Basic Input Output System) firmware.

What is particularly-concerning is the possible ripple effect this attack may have. As part of the attack, private Intel Boot Guard keys were leaked for 116 MSI Products. Intel Boot Guard is a security feature in modern Intel hardware that prevents malicious firmware from loading before the operating system. This feature is crucial, as malicious firmware can hide activities from security and antivirus software and persist even after OS reinstallation.

As leaked keys are believed to be built into Intel hardware. They may not be able to be modified and, therefore, with the leaked keys the attackers can bypass Intel Boot Guard and install malicious software, before the operating system is able to identify, quarantine, and remove it.

If this proves to be the case, this attack showcases the dangers of supply-chain attacks and the importance of verifying that your suppliers adhere to an appropriate level of cybersecurity.

THREAT FEATURE:
ISLE OF MAN GOVERNMENT

The Isle of Man Government is a large user of digital technology to aide the delivery of Government services across the island, and with a large and diverse workforce is a prime target for cyber threats. Government is continually reviewing the cyber security landscape to understand current and future threats. Various types of security measures are deployed to ensure the integrity of the Government network and the security of the data processed on it.

As with other large organisations, one of the biggest threats is caused by phishing emails and the sheer quantity of spam emails and the potential malware contained within. Systems are in place to identify and remove emails which are identified as spam or phishing attempts before they reach a users mailbox, and on average stop the delivery of approximately 500,000 spam emails per month.

Regular awareness training and staff bulletins ensure that Government users are aware of the risks around all forms of cyber-attack, whether that be by email, direct cyber-attacks or forms of social engineering including impersonation on social media channels.

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 Office of Cyber-Security & Information Assurance (OCSIA) was established by a Council of Ministers Directive in October 2017. In March 2023 we established the Cyber Security Centre for the Isle of Man (CSC) which is our public facing body providing advice, guidance and practical support to Island residents and businesses.

The CSC acts as the focal point in developing the Island's cyber resilience, working in partnership with private and third sector organisations across the Island alongside the wider population. As a part of OCSIA the CSC works in the public sphere whilst OCSIA focuses on Information assurance within Government.

We are committed to supporting Island-residents and businesses by providing practical and targeted advice and guidance. This includes working in partnership with the private sector to improve their cyber resilience and raise awareness about the latest cyber threats affecting our Island.

OCSIA also hosts an annual conference 'CYBERISLE' which is held over the course of one day, and helps business leaders, individuals, community and charitable organisations understand the rapidly changing cyber-security threat landscape.

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

www.ocsia.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