NFIB Special Operations
Cyber Monthly Threat Update – August 2023

Welcome to the new Cyber Monthly Threat Update for the City of London Police. This document provides an overview of cybercrime trends using Action Fraud data for the period 1st – 31st August 2023.

Contact: If anyone has any information they wish to put forward to be considered for this document, please contact the Cyber Intelligence Team on: NFIB Cyber Intel NFIB-CyberIntel@cityoflondon.police.uk

Overall Reporting	ECRS	Subject Areas

Contents:

A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

CITY of LONDON POLICE

Key Findings

- Cyber Crime reporting figures have significantly decreased in August. 2,378 reports were received, representing a 19% decrease on the 2,923 reports in July. This was due to a drop in reports of social media hacking, which fell by 17.3% this month.

- Social media hacking continues to account for most of the Cyber Crime reported to Action Fraud, with 1,392 reports received in August, accounting for more than half of all cyber reports (58.5%).

- Social Media Takeovers leading to incidents of online shopping and ticket fraud have increased in August. It is almost certain that offenders who were previously only using hacked account to promote fraudulent investments have adapted to commit online shopping and ticket fraud as a more reliable method of monetization. Primarily, Taylor Swift tickets are being advertised on the victim's hacked account.

- The WhatsApp vishing method has adapted slightly in August with the hook used by offenders changing, with suspects claiming to be from job sites explaining the need for the victim to share their six-digit code for joining a call about this job opportunity.

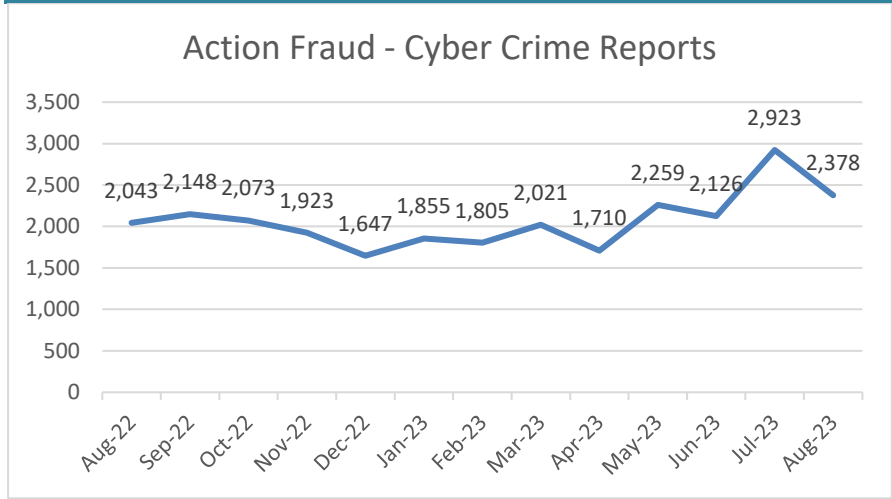
- Organisations mostly reported business email compromise (BEC) or ransomware incidents. This is a slight change from July, where hacking made up the second most common reported offences. This is a return to more normal patterns of reporting.

- Retail/Trade was the highest reporting single sector in August, with Education falling from top in July to 12th in August, due to summer holidays.

- Insider Threats were the most reported attack vector method in August. This is far more than usual and is driven, primarily, by disgruntled former employees who retained access to systems or ex-partners using social engineering to alter permissions.

- Three new variants, 'INC', '8base', and 'Rorsach/BabLock' were identified in August 2023, although 8base is said to have first come on the ransomware scene in March 2022.

Overall Reporting



- 62.4% (1,484) of reports were classified as cyber-dependent, with 18.6% (443) classified as cyber-enabled.

Enhanced Cyber Reporting Service (ECRS)

- Business Email Compromise (BEC) was the highest reported fraud in August, accounting for 35%, Ransomware was the second most reported and Hacking was third with 17%. This is a return to more normal patterns of reporting after BEC and Hacking experienced near identical reporting volumes in July.
- The most common type of BEC reported was Invoice fraud, significantly more than the second most reported form – CEO Fraud.
- Within BEC the most identified attack vector was Phishing or stolen/spoofed credentials, however in the majority of reports the attack vector could not be identified. It is assessed that the majority of the unidentified attack vectors will be some form of credential compromise through phishing.
- Reports of Ransomware increased in August with Medium sized companies (employing between 50 and 249 employees) responsible for the highest volume of reports.
- Social media continued to be the most targeted resource in cases of Hacking.
- Insider Threat was by far the most reported attack vector method. This is far more than usual for insiders and is driven, primarily, by disgruntled former employees who retained access to systems or ex-partners using social engineering to alter permissions.
- As in July, Micro businesses (1-9 employees) were the principal reporters, attributable to 25% of cases.
- Retail/Trade was the highest reporting single sector, accounted for 10% of reports with Education falling from top in July to 12th in August – this is assessed to be due to summer holidays. Construction and Manufacturing made up the top three industries, accounted for 9% of reports each.

Variant	No. of Reports
Akira	5
Lockbit 2.0	3
Ragnar locker	2
INC	2
Phobos	2
Lockbit 3.0	1
Cactus	1
Monti	1
Rorscach	1
Blackcat/ALPHV	1
Cl0p	1
8base	1
Total	**21**

Subject Areas

Ransomware

- 45 ransomware reports to Action Fraud were identified in August 2023, which is an increase compared to the previous 3 months, which stood at 31, 32 and 34 respectively.
- Three new variants, 'INC', '8base', and 'Rorsach/BabLock' were identified in August 2023.8base is said to have first come on the ransomware scene in March 2022, but "with a significant spike in activity in the summer of 2023, cyber security experts state[1]. However, currently, there is not enough information available to determine how big or small the group is, where the suspects are located, or if 8BASE is backed by any nation-state entities or governments.
- In August, both Akira and Lockbit were the most reported variants, with 4 reports.
- In August, 'Other service activities' was the most targeted sector, with 13 reports.
- Businesses with 50 – 249 employees were the most likely to report a ransomware attack making up 33% of reporting.

Phishing

Phishy Friday Alerts:

In August, two Phishy Friday alerts were sent out. The Phillips Air Fryer phishing email stated that the recipients of the email had won the item and asking for personal details to claim their prize. The McAfee Total Protection email informed recipients that their protection had expired, and their computers were at risk. Recipients were given a link asking them to 'renew now'.

Trends:

- An emerging MO detected in August was an evolution of the common sextortion email, whereby suspects had claimed access to the victim's devices and had video footage of them watching adult materials. The new adaptation of the sextortion email now includes explicit images within the email, which claim to be of the

[1] 'Who is 8BASE? A deep dive into the "newish" ransom gang' | Cybernews

victims, however the same images are used in multiple emails. The email subject is “You have a new message” and there were 450 of these emails detected in August, with 32.44% of those being malicious.

Emerging Trends:

- Electricity bills – a recent phishing scam has circulated regarding eliminating electricity bills, asking victims to click on a link and enter personal information to “see if you qualify”. 762 emails were reported in August, and the MO could evolve to include heating bills as the months get colder.
- Wilkos – phishing emails relating to the closure of Wilkos/Wilkinson was an emerging trend this month. There were a small number of reports made so this MO is ongoing and being monitored.
- RyanAir – holiday phishing scams could be on the rise, with fraudsters targeting individuals who are looking to book cheap summer holidays for next year. People could be susceptible to this phishing scam due to the ongoing cost of living crisis.

Hacking: Social Media and Email

Reporting:

Overall reporting of social media hacking has decreased in August from the record figure in July, falling by 17.3%. This figure is an increase when compared to June as well as last year, indicating a sustained rise in reporting of SMH.

There have been no significant changes in the most identified methods nor motives of social media hacking. Across the different platforms identified in reporting, offenders have continued to follow the methodologies they have been successful with over the last 15 months.

Trends:

The WhatsApp vishing method, subject to two alerts by Action Fraud, has adapted slightly in August. It is possible this is in response to the Action Fraud alert specifically mentioning the target of religious WhatsApp groups. In August, the hook used by offenders has changed, with suspects claiming to be from job sites, most often jobs in security, and will explain the need for the victim to share their six-digit code as required for joining a call about this job opportunity.

There has also been a minor increase in social media hacking incidents leading to online shopping fraud being committed by a suspect using the victim’s hacked account. This is particularly concerning as many victims as possible of these takeovers suffer threats and harassment by those defrauded by the offender now impersonating the victim on their account. In a small number of incidents, the offender has sold fake Taylor Swift tickets on the victim’s account.

Distribution List

Organisation	Department / Role	Name
Public		

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018.

The cover sheets must not be detached from the report to which they refer.

Protective Marking	Official – Public
FOIA Exemption	No
Suitable for Publication Scheme	No
Version	Final
	Cyber Intelligence Team
Purpose	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.
Owner	CoLP
Author	Cyber Intelligence Team
Reviewed By	Cyber Intelligence Team

CITY OF LONDON POLICE