National Cyber Security Centre

Active Cyber Defence

The 6th Year: Summary of Key Findings

Contents

What is Active Cyber Defence?

www.ncsc.gov.uk/acd

The aim of Active Cyber Defence (ACD) is to "Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time." It was launched in 2017 and continues to protect the UK, in a relatively automated way, from a significant proportion of commodity cyber attacks.

The ACD programme is one of the NCSC's most successful projects to counter online threats, reducing high-volume attacks (such as malware) from ever reaching UK citizens whilst removing the burden of action from the user. Its core services include Takedown, Protective DNS, Early Warning and Exercise in a Box.

This document summarises some of the key findings from the sixth year of the ACD programme. A fuller report, covering all of the services within the ACD programme, will be published shortly.

Takedown Service

www.ncsc.gov.uk/information/takedown-service

The Takedown Service finds malicious sites and sends notifications to the host or owner to get them removed from the internet before significant harm can be done. The NCSC centrally manages the service, so government departments automatically benefit without having to sign up.

We define 'attacks' and 'attack groups', the major distinction being how we count associated URLs related to a single campaign into a group:

- an 'attack' is a single URL involved in a campaign
- an 'attack group' is how we refer to all the URLs that form part of a campaign

Key findings from the Takedown Service

There had been significant year-on-year growth in the total number of takedowns conducted by the Takedown Service since it was introduced in 2017, but in 2022 there was a drop:

- the total takedowns by campaign group, which had risen to 2.7 million in 2021 (from 700,000 in 2020) fell to 1.8 million in 2022
- similarly, the total URLs, which had risen to 3.1 million in 2021 (from 1.45 million in 2020) fell to 2.4 million in 2022

Most of the reduction in takedowns can be attributed to extortion mail servers (down 528,000) and cryptocurrency investment scams (down 459,000), whilst the frequency of other attack types has either grown or remained static.

These two attack types have some of the shortest uptimes on average, which could explain the reduction in prevalence as attackers concentrate on areas where their return on investment is greater. Mail servers and cryptocurrency investment scams have a median availability of 25.5 and 1 hour respectively. The next top 5 attack types are fake shop, phishing URL, brute force attack, web shell and malware infrastructure URL. Contrastingly, they have a combined median of 56.29 hours.

Cryptocurrency investment scams

We started takedowns against this attack type in 2020 due to the large numbers observed. Figure 1 shows that takedowns peaked in January 2021, with a consistent downward trend thereafter.

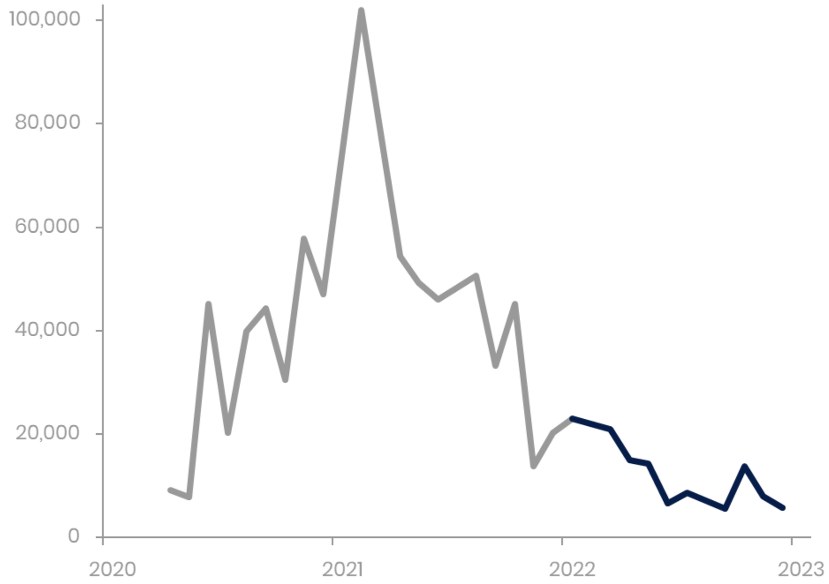
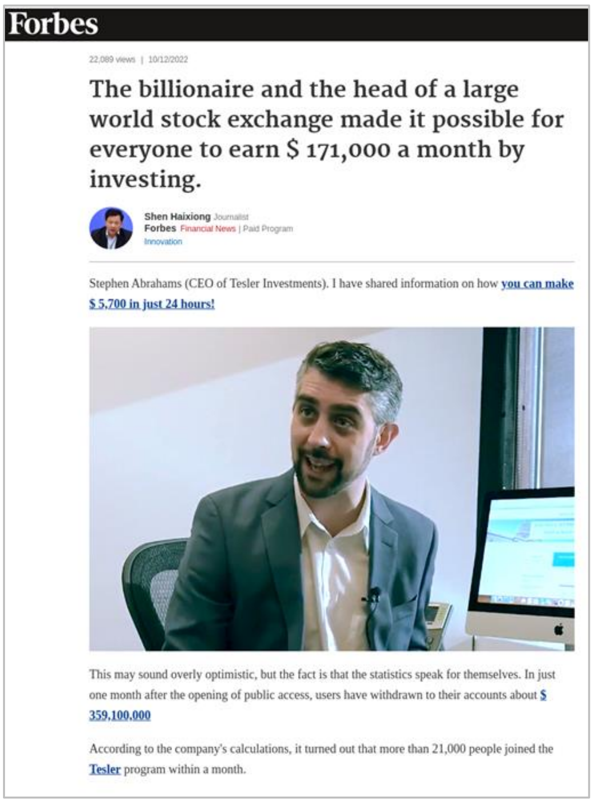


Figure 1 Cryptocurrency investment scams taken down 2020-2023

Despite the fall in takedowns, cryptocurrency investment scams continue to be a high-volume attack type. These attacks usually use celebrities or well-known brands to appear legitimate.



Forbes

22,089 views | 10/12/2022

The billionaire and the head of a large world stock exchange made it possible for everyone to earn $ 171,000 a month by investing.

Shen Haixiong Journalist
Forbes Financial News | Paid Program
Innovation

Stephen Abrahams (CEO of Tesler Investments). I have shared information on how you can make $ 5,700 in just 24 hours!

This may sound overly optimistic, but the fact is that the statistics speak for themselves. In just one month after the opening of public access, users have withdrawn to their accounts about $ 359,100,000

According to the company's calculations, it turned out that more than 21,000 people joined the Tesler program within a month.

Image 1 Investment scam example

Government-themed scams

Attacks on the HMG brand decreased 17% from 2021, whereas attacks on other parts of UK IP space grew 26%. Attacks on HMG brands tripled during the pandemic but have now returned to pre-COVID levels. Figure 2 shows the top UK government brands used in phishing attacks, and the reduction we have seen over the last 2 years.

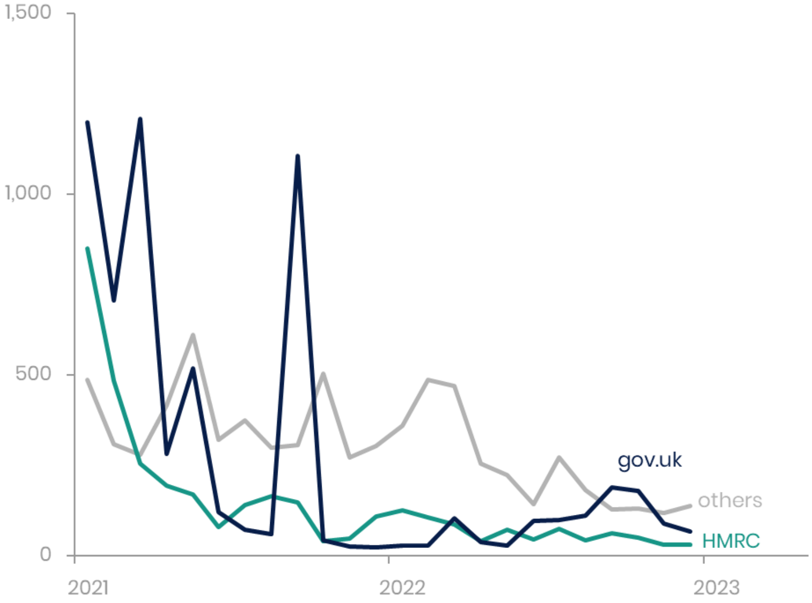
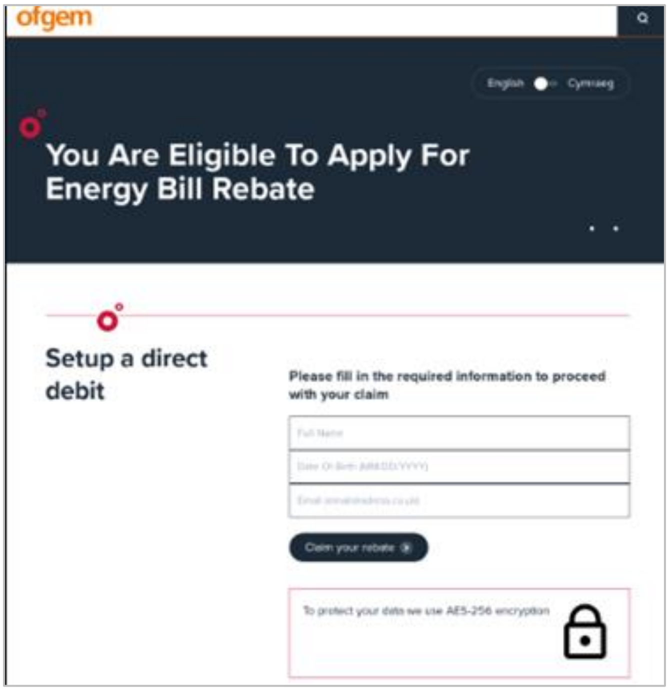


Figure 2 UK government brands used in phishing attacks 2021-2022

Energy bill scams

Criminals continue to exploit topical events to make phishing attempts more convincing, in this case targeting vulnerable people. In September and October 2022, we saw an influx of phishing attempts targeting the UK government's Energy Bills Support Scheme. These URLs typically included keywords such as 'rebate', 'grant' and 'scheme' to sound legitimate.



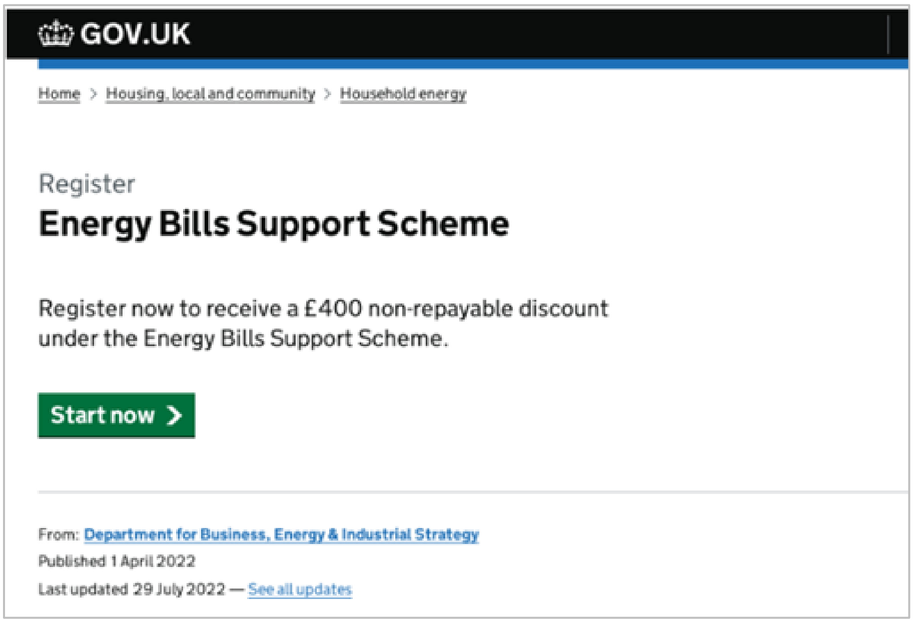
You Are Eligible To Apply For Energy Bill Rebate

Setup a direct debit

Please fill in the required information to proceed with your claim

To protect your data we use AES-256 encryption

Image 2 Energy bill scam example 1



Register

Energy Bills Support Scheme

Register now to receive a £400 non-repayable discount under the Energy Bills Support Scheme.

From: Department for Business, Energy & Industrial Strategy
Published 1 April 2022
Last updated 29 July 2022 — See all updates

Image 3 Energy bill scam example 2

Web shells

Web shells are created by attackers using malicious scripts to install control panels on compromised servers. These servers can then be used as a launch pad for malicious activity such as hosting phishing sites.The number of web shells we have discovered and acted against increased in 2022 by around 15%. The most prevalent hosting providers of web shells were Newfold Digital, Cloudflare and GoDaddy.

Suspicious Email Reporting Service (SERS)

www.ncsc.gov.uk/collection/phishing-scams

The Suspicious Email Reporting Service (SERS) enables the public to report suspicious emails and websites to the NCSC. These reports are sent on to our takedown provider for analysis, and when links to malicious sites are found, we seek to remove those sites from the internet to prevent them doing further harm.

Key findings from the Suspicious Email Reporting Service

In 2022, SERS received over 7.1 million reports from members of the public, an average of over 19,500 a day. This is an increase of over 33% on the number of reports received in 2021.

SERS reports were responsible for the removal of over 72,000 malicious URLs across 40,000 scam campaigns in 2022. Malicious URLs reported to SERS were removed from the internet, on average, within 6 hours.

Over 96% of reports are received via email. The remainder are from a combination of the NCSC website form and O365 'report phishing' function (see https://www.ncsc.gov.uk/guidance/configuring-o365-outlook-report-phishing-for-sers for details).

Mail Check

www.ncsc.gov.uk/information/mailcheck

Mail Check is the NCSC’s platform for assessing email security compliance. It helps domain owners identify, understand, and prevent abuse of their email domains. Mail Check supports organisations to implement the following controls:

- email anti-spoofing controls (SPF, DKIM, and DMARC): these standards help prevent various attacks (for example, phishing) that use an organisation's email domain to trick email recipients
- email confidentiality (TLS and MTA-STS): keeping messages encrypted and private as they are sent over the internet

Key findings from Mail Check

Mail Check is a mature service with an established user base that continues to grow. 2022 saw an increase in the number of organisations using the service, up to 2,452 from 1,530 at the end of 2021. This was primarily driven by an uptake across universities, colleges and schools (up to 1,258 from 515), and charities (up to 410 from 188). The number of domains in Mail Check nearly doubled in 2022, growing from around 29,000 to over 54,000. 63% of these new domains belonged to schools.

DMARC adoption in the UK public sector

To make a domain as difficult to spoof as possible, the NCSC recommends the use of DMARC with an enforcing policy of either ‘reject’ or ‘quarantine’.

In 2022, we reached the landmark of 100% of all central government departments adopting a strict DMARC policy (up from 91% at the end of 2021), which means that email coming from central government is now hard to spoof.

In the previous 30 days before publication of this report, we saw over 80 million spoofed emails blocked from these central government domains, as a direct result of strict DMARC implementation.

In total, 1,124 domains progressed from non-existent (or non-enforcing) policies to enforcing ones in 2022, notably in the devolved administrations and Crown Dependencies.

Email Security Check

Email Security Check (ESC) is the lightweight version of Mail Check which is publicly accessible. ESC provides a quick and simple way of conducting email security checks, and acts as a gateway to other NCSC services and tools (such as Mail Check and commercially provided alternatives). Since its launch at CYBERUK 2022, ESC has scanned over 54,000 email domains.

Vulnerability Checking

In the last year, the NCSC has been consolidating its vulnerability checking services onto a common technical platform. Our website security testing service – Web Check – along with other vulnerability checking capabilities are being combined in our MyNCSC service. We have also added new capability to check for many of the vulnerabilities on CISA's Known Exploited Vulnerabilities list. We will continue to develop this flagship service to add checks for other types of vulnerabilities over the coming year.

Whilst the above set of capabilities requires registration and onboarding for organisations, we identified a need for a simpler vulnerability checking service to help smaller organisations in particular, without the need for a user to create an account. We have therefore developed a radically simple service 'Check Your Cyber Security' to provide some of the most important vulnerability checks. The service allows users to find and fix some of the most important cyber security issues without requiring ongoing support from NCSC.

Check Your Cyber Security is geared towards empowering non-technical users to fix their vulnerabilities by exploiting NCSC's data and expertise, at scale.

Key findings from Vulnerability Checking

Web Check

The Web Check customer base grew by approximately 1,000 users during 2022, an increase of 26%. The number of unique URLs and domains being scanned increased by 33%. The service presented over 12,000 'urgent findings' to users, of which 95% have been resolved.

Check Your Cyber Security

Web Check is only available to certain sectors. After conducting extensive user research to identify the cyber security challenges that SMEs face, we introduced a public product, Check Your Cyber Security. The first iteration addresses vulnerabilities and configuration errors which are present in over 370,000 computers and servers in the UK, and which can be exploited by cyber security attacks (such as ransomware). It also includes a Browser Check to identify the millions of UK devices that are not running the latest browser version (and are therefore vulnerable).

Protective Domain Name Service (PDNS)

www.ncsc.gov.uk/information/pdns

The Domain Name System (DNS) is the known as ‘the address book of the internet’. Your computer relies on DNS to find out exactly where ‘Example Domain’ (a domain) is located (its IP address), so it can connect to it. Anyone can register a domain so that everyone else can find the IP address to connect to it. Unfortunately, attackers often use seemingly legitimate domains as part of malware and phishing attacks. The NCSC’s Protective DNS (PDNS) service exists to combat that malicious activity for public sector users. It prevents the successful resolution of domains associated with malicious activity, while enabling the rest of the internet to remain accessible.

Key findings from Protective DNS

PDNS has continued to grow in terms of number of UK organisations it protects, the number of queries and blocks it performs, and the protection it offers to from online threats.

In 2022, the number of organisations using PDNS grew by 24% from 944 to 1,173. Note this figure does not include NHS trusts (which benefit from PDNS) because we provide the service at a national level rather than to individual NHS organisations.

In 2022:

- PDNS queries grew by 29% from 66 billion to 86 billion per month
- PDNS handled 0.55 trillion DNS queries, and blocked 11 billion DNS queries for 420,000 domains, corresponding to 2% of all queries
- PDNS blocked over 5 million requests for domains associated with ransomware, a significant contribution to protecting UK organisations from this threat
- the most blocked, attributable threats were Cobalt Strike, Flubot, CryptoStealer and SocGholish

We have continued to grow the PDNS community to better understand the needs of our users, progressing their key priorities of protecting roaming devices and identifying which devices had DNS queries blocked. We are currently developing integration tools that will make it easier to ingest PDNS data into the most popular SIEM tools.

Exercise in a Box

www.ncsc.gov.uk/information/exercise-in-a-box

Exercise in a Box (EiaB) is a publicly available tool that allows organisations to practise and refine their response to the most pressing cyber security incidents in safe and private environment.

Facilitators are given the tools they need to lead relevant staff within their organisation through a scenario that unfolds through a series of prompts. This is designed to stimulate discussion about an organisation's policies, processes and procedures, with attendees self-assessing their organisation's maturity and readiness against a sliding scale.

At the end of the exercise, a downloadable 'End Report' is created, which includes links to relevant NCSC advice and guidance. Primarily aimed at the non-technical audience within both the public sector and SMEs, the service has also seen strong take-up amongst large organisations and cyber security professionals.

Key findings from Exercise in a Box

By the end of 2022, just over 18,500 users worldwide were using EiaB, an increase of around 40% on 2021. The largest increase in signups was from large businesses, up 61%. Signups by cyber security professionals were up 50%, those from public sector were up 37% and small organisation signups were up 36%.

Early Warning

www.ncsc.gov.uk/information/early-warning-service

Early Warning is a free NCSC service designed to automatically inform an organisation of potential cyber attacks on their network, as soon as possible. The service uses a variety of information feeds from the NCSC, and trusted public, commercial and closed sources (which includes several privileged feeds which are not available elsewhere). Early Warning filters millions of events that the NCSC receives every day and - using the IP and domain names provided by our users - correlates those which are relevant to their organisation into daily notifications for their nominated contacts.

Key findings from the Early Warning service

Any UK organisation with a static IP address or domain name can sign up to use Early Warning. In 2022, 2,939 new customer organisations signed up to the service, a 38% increase on the previous year, with a total of 7,819 organisations at end of 2022.

- 570 organisations were warned about active malware on their networks
- 2,270 were warned about vulnerabilities on their networks
- 1,193 were warned about a host on their network scanning the internet, which might be, for example, an indicator of a possible compromise.

In 2022, Minerpanel, Avalanche and CobaltStrike were the infections reported on the largest number of Early Warning customer organisations. Ramnit, Citeary and Saility were found on the most IP addresses in total (whether those IPs belonged to an Early Warning customer or not).