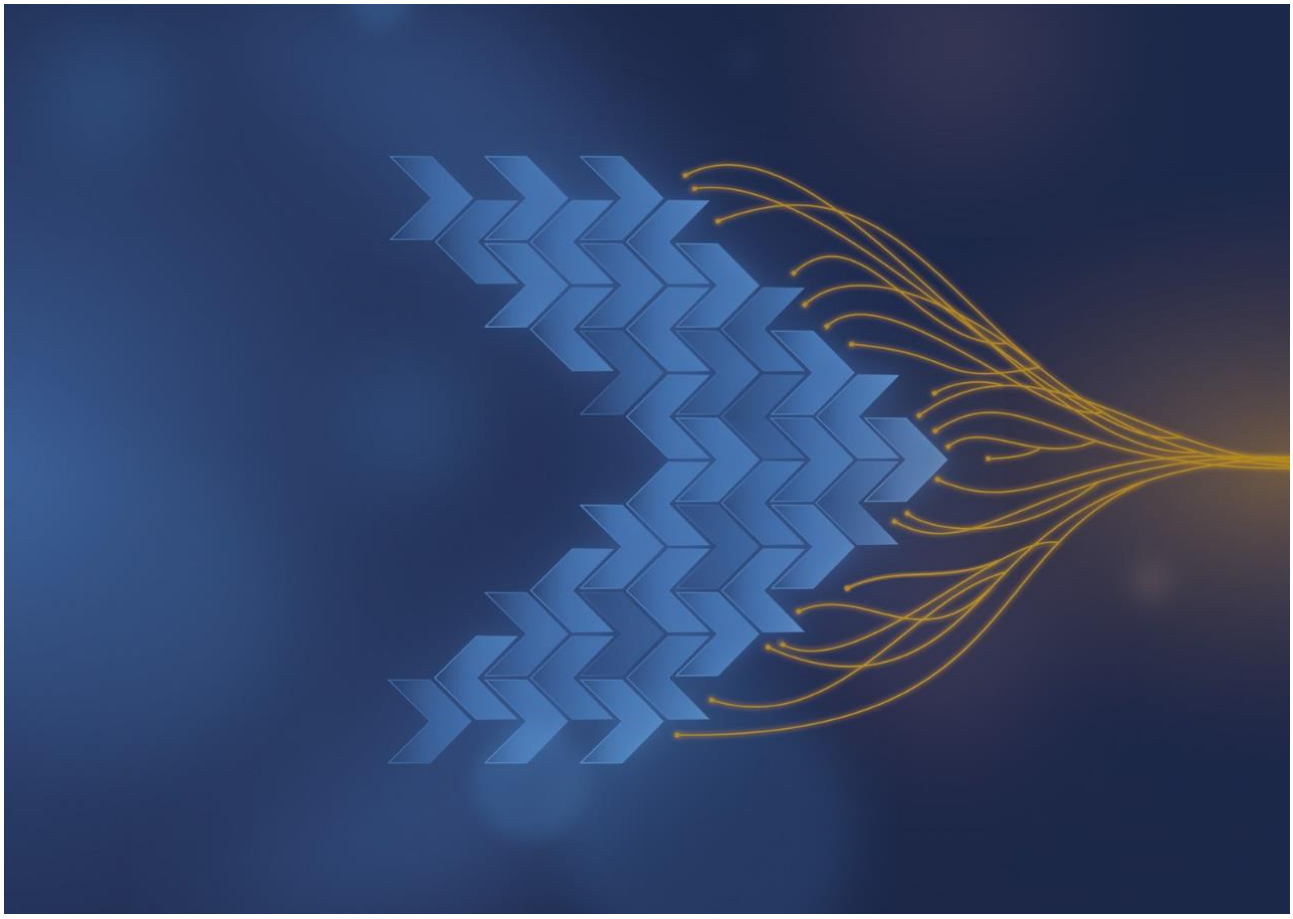
National Cyber Security Centre



Active Cyber Defence

The 5th Year: Summary of Key Findings

Contents

What is Active Cyber Defence?

www.ncsc.gov.uk/acd

The UK continues to be one of the most digitally advanced countries in the world, with our lives being online more than ever before. As this digitisation continues, it is vital that the UK remains able to protect its organisations, business and citizens against cyber crime.

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 ways to help bring about a real-world, positive impact against threats. The programme seeks to reduce high-volume cyber attacks, such as malware, ever reaching UK citizens, and aims to remove the burden of action from the user.

The ACD programme's core services include Takedown, Protective DNS, Early Warning and Exercise in a Box. **This document summarises some of the key findings from the fifth year of the NCSC´s 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 departments automatically benefit without having to sign up.

Key findings from the Takedown Service

In total, 2.7M campaigns (3.1M URLs) were taken down in 2021. This is a significant increase when compared with 2020's tally (700,595 campaigns and 1,448,214 URLs) and is principally due to the prolonged period we have been performing takedowns against extortion mail server and celebrity-endorsed investment scams throughout 2021. These attacks are widely distributed and generate a proportionally large number of takedown records.

Table 1: Total takedowns by attack campaign group, 2020 and 2021

Attack Type	2020	2021
Extortion Mail Server	179,008 (Nov-Dec)	1,867,435
Celeb Endorsed Investment Scams	290,345 (Apr-Dec)	607,723
Fake Shop	160,295 (Apr-Dec)	107,251
Phishing URL	33,964	54,382
Web Shell	5,323	26,060
Advance Fee Fraud	27,346	19,197
Technical Support Scam	1,450 (Nov-Dec)	14,448
Advance Fee Fraud Mail Server	2,686	6,632
Malware Infrastructure URL	4,755	4,668
Vulnerable Application	-	4,050
Phishing URL Mail Server	6,849	53,437
Malware Attachment Mail Server	7,839	2,580
Malware Distribution URL	5,198	2,188
Malware C2 IP	880	1,767
Web-Inject Malware URL	1,616	1,358
Fake Pharmacy	797	881
Shopping Site Skimmer	1,505	875
Instagram Brand Infringement	266	723
Insta Malware Command and Control Centre	720	682
Facebook Brand Infringement	65	327
Clone Firm Email	161 (Nov-Dec)	319 (Jan-May)
Clone Firm URL	132	224
Twitter Brand Infringement	38	206

Attack Type	2020	2021
Cryptocurrency Miner	135	133
Survey or Affiliate Scam	-	133
Phishkit Archive	150	117
TikTok Brand Infringement	-	71
Fake Mobile App	67	11,867
Other URL	6	65
Advance Fee Fraud Phone Number	186 (Nov-Dec)	65 (Jan-June)
DKIM Signed Email Domain	314	64
Clone Firm Phone Number	124	45
Brand Infringement	33	44
Skimmer Credential Dropsite	66	33
Technical Support Scam Number	-	32
JavaScript Resource	74	24
Phishkit Email	84	18
Fraudulent Use of PayPal on Fake Shops	-	12
Telegram Brand Infringement	-	8
Fake Bank URL	4	4
Phishing Dropsite	4	4
WhatsApp Brand Infringement	3	2
Other Phone Number	1	42
Other Email	3	2
Business Email Compromise	-	1
Fake Bond Comparison Site	-	1
Google Adwords	-	1
Malware URL Mail Server	11	0
Defaced Website	4	0
LinkedIn Impersonation	3	0
Malware Payment URL	3	0
Code Repository Sensitive Data	2	0
Credential Drop URL	2	0
Domain	1	0
Targeted Attack	1	0

Government-themed scams

In 2021, we took down 11,001 phishing campaigns, a total of 49,228 URLs with a median availability of 14 hours. The median availability of these campaigns was 5 hours shorter than in 2020, meaning they had less time to do harm.

Table 2 Top 10 UK government-phished brands

Government brand	Number of attack URLs	Number of attack groups (campaigns)	Median availability (hours)
Generic 'gov.uk'	18,037	5,257	15
HMRC	12,516	2,592	11
NHS	5,513	1,405	8
TV Licensing	4,412	1,089	154
DVLA	6,418	1,013	17
Office for National Statistics (Census theme)	572	354	1
Government Gateway	1,334	267	21
BBC	103	51	20
Council Tax	94	39	3
Generic 'HMG'	29	27	30
All UK government-themed phishing attacks	**49,228**	**11,001**	**14.3**

NHS and vaccine-themed campaigns

The first campaigns to use the NHS vaccine lure were noted in late December 2020 and were delivered in email and SMS campaigns with over 70 throughout January 2021. These attacks tailed off in numbers until summer when vaccine certification became a popular topic for lures.

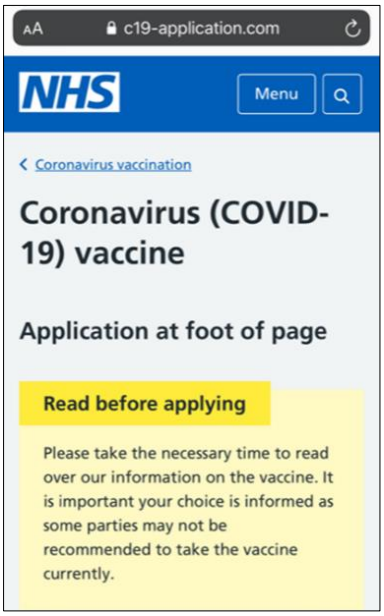


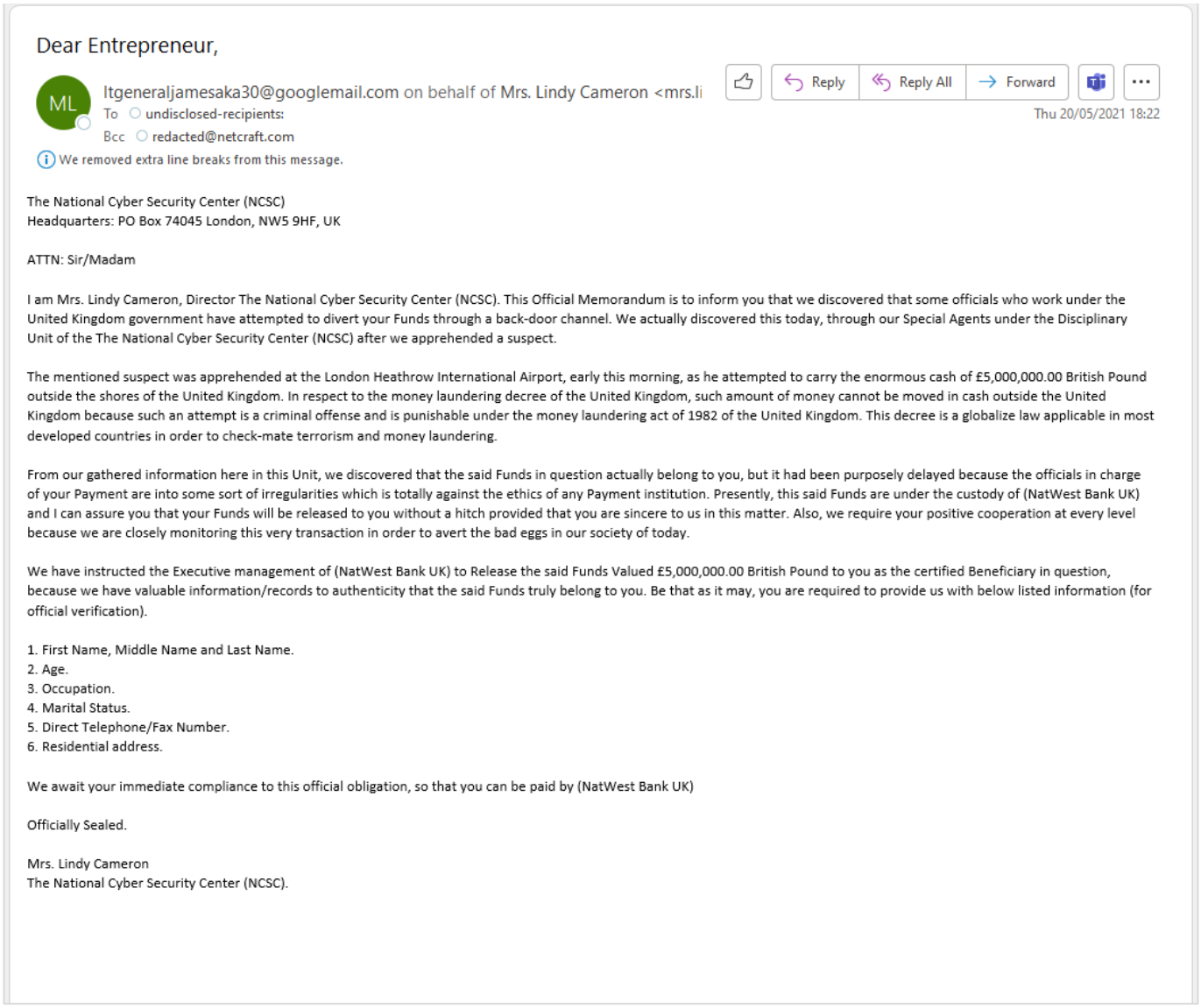
Figure 1 Fake NHS COVID-19 Vaccine Booking (January 2021)

Figure 2 Fake NHS Digital Vaccine Passport Phishing (June 2021)

These campaigns were designed to harvest personal and financial information from victims. The phishing sites falsely offered vaccine booking appointments in return for a small 'fee', but as is common with other phishing campaigns, personal and financial information posted into these phishing forms was subsequently used by phishers to enable further fraud, often contacting victims directly purporting to be from UK banks.

By summer 2021, criminals modified the campaign to offer fake vaccine passports, which falsely claimed to support international travel requirements. Some even provided a QR code which looks authentic but when scanned simply redirected the victim to a free QR code generation site.

Even the NCSC was not immune from being used as a lure in a campaign, as the following advanced fee fraud example shows. Advanced fee fraud is when fraudsters target victims to make advance or upfront payments for goods or services that do not materialise.



Dear Entrepreneur,

ML

ltgeneraljamesaka30@googlemail.com on behalf of Mrs. Lindy Cameron <mrs.li

To undisclosed-recipients:

Bcc redacted@netcraft.com

Reply | Reply All | Forward

Thu 20/05/2021 18:22

We removed extra line breaks from this message.

The National Cyber Security Center (NCSC)
Headquarters: PO Box 74045 London, NW5 9HF, UK

ATTN: Sir/Madam

I am Mrs. Lindy Cameron, Director The National Cyber Security Center (NCSC). This Official Memorandum is to inform you that we discovered that some officials who work under the United Kingdom government have attempted to divert your Funds through a back-door channel. We actually discovered this today, through our Special Agents under the Disciplinary Unit of the The National Cyber Security Center (NCSC) after we apprehended a suspect.

The mentioned suspect was apprehended at the London Heathrow International Airport, early this morning, as he attempted to carry the enormous cash of £5,000,000.00 British Pound outside the shores of the United Kingdom. In respect to the money laundering decree of the United Kingdom, such amount of money cannot be moved in cash outside the United Kingdom because such an attempt is a criminal offense and is punishable under the money laundering act of 1982 of the United Kingdom. This decree is a globalize law applicable in most developed countries in order to check-mate terrorism and money laundering.

From our gathered information here in this Unit, we discovered that the said Funds in question actually belong to you, but it had been purposely delayed because the officials in charge of your Payment are into some sort of irregularities which is totally against the ethics of any Payment institution. Presently, this said Funds are under the custody of (NatWest Bank UK) and I can assure you that your Funds will be released to you without a hitch provided that you are sincere to us in this matter. Also, we require your positive cooperation at every level because we are closely monitoring this very transaction in order to avert the bad eggs in our society of today.

We have instructed the Executive management of (NatWest Bank UK) to Release the said Funds Valued £5,000,000.00 British Pound to you as the certified Beneficiary in question, because we have valuable information/records to authenticity that the said Funds truly belong to you. Be that as it may, you are required to provide us with below listed information (for official verification).

1. First Name, Middle Name and Last Name.
2. Age.
3. Occupation.
4. Marital Status.
5. Direct Telephone/Fax Number.
6. Residential address.

We await your immediate compliance to this official obligation, so that you can be paid by (NatWest Bank UK)

Officially Sealed.

Mrs. Lindy Cameron
The National Cyber Security Center (NCSC).

Figure 3 NCSC-themed advance fee fraud, where the fraudster claims to be CEO NCSC Lindy Cameron

Fake celebrity endorsement scams

We started these takedowns in 2020 and they have continued to be a widespread attack promoted in spam, SMS and via online adverts. As before, none of the celebrities featured in these scams are aware or involved in any way. During 2021 we took down 319,365 campaign groups (607,723 URLs). These attacks had a median attack availability of just 1 hour.

Figure 4 Example of fake celebrity endorsement scams

Throughout 2021, the monthly takedown totals for this type of scam have shown a downward trend.

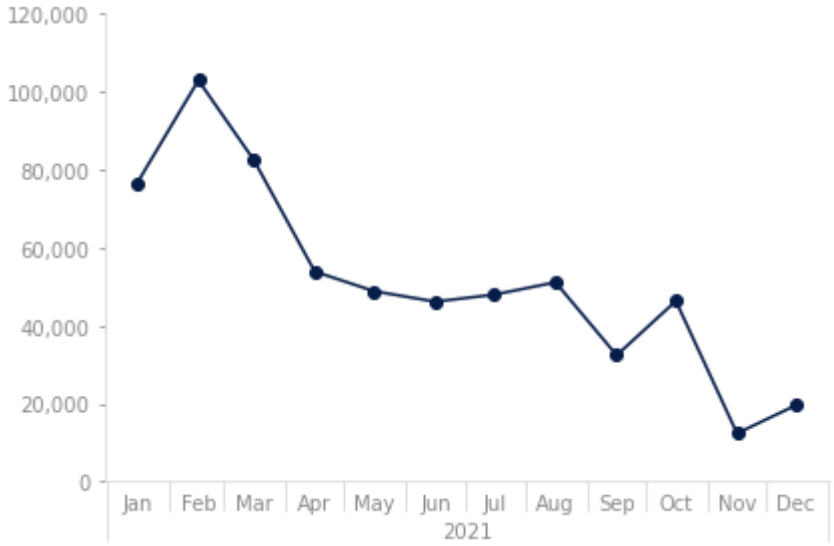


Figure 5 Celebrity endorsed scams in 2021 by campaign groups

Extortion mails

Like the celebrity endorsed scams, the extortion mail server takedowns are another example of a very prevalent attack which many readers may recognise. These attacks falsely claim that recipients have been hacked and some will attempt to add authenticity by quoting a password which a recipient may recognise. These passwords are often derived from publicly pasted breaches which the recipient may not realise they were part of. The mail urges recipients to purchase and send cryptocurrency to a crypto wallet or risk the release of 'compromising' material.

In 2021, we took down 1.87M servers sending these attacks with a median attack availability of 26 hours. Looking at the hosting of these servers we can see that they are widely distributed across the internet. The top 10 hosters of extortion mail servers in 2021 are below.

Table 3 Top 10 hosters of extortion mail servers in 2021

Hoster	Total Groups	Percentage of Campaigns
Bharti Airtel	156,516	8.4%
PTCL	101,788	5.5%
Vodafone Group	57,436	3.1%
Telefonica	52,092	2.8%
iam.ma	31,736	1.7%
ideacellular.com	28,084	1.5%
America Movil	27,082	1.5%
Antel	21,487	1.2%
Hathway Cable & Datacom	21,316	1.1%
Deutsche Telekom	21,193	1.1%

Remote access trojans

Remote access trojans (RATs) are used by attackers to conduct more detailed reconnaissance of a victim device or network. These provide a backdoor to enable other capabilities, which an attacker could subsequently deploy.

In 2021, we were able to take down 5,944 instances of infrastructure used for RAT distribution and command and control (9,069 URLs). This is a large increase on last year's total of 1,733 (2,954 URLs). The main reason for this increase is due to improvements in detection and monitoring of these attacks. The median availability increased this year from 39 hours to 106 hours. Cobalt Strike C2 was the most prevalent RAT in our takedowns this year with a 60% share.

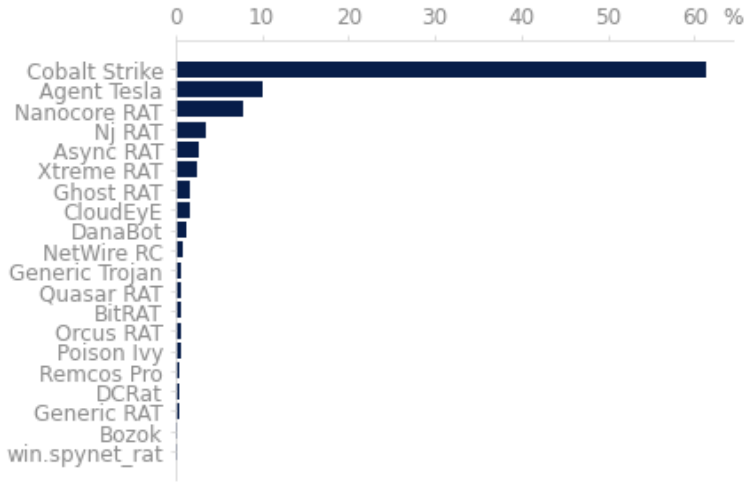


Figure 6 Remote access trojan takedowns by prevalence in 2021

Protective DNS

www.ncsc.gov.uk/information/pdns

Protective DNS (PDNS) prevents users from accessing domains or IPs that are known to contain malicious content and stops malware already on a network from calling home. The user base now covers significant portions of central government, local government, law enforcement and health sector, and the threats we face have changed. Back in 2017 we were often blocking DNS requests to domains associated with Wannacry, BadRabbit, Ramnit and Conficker, whereas today we are more likely to block domains associated with Ryuk, Conti, FluBot, Monerominer (and still Conficker).

Key findings from Protective DNS

In 2021, PDNS handled more than 602 billion DNS requests. Of these, over 160 million requests were blocked. Our sources tell us that the most common reason for blocking a request was because the domain was associated with FluBot, Conficker, Monerominer, Ryuk, Doubleback, CobaltStrike Beacon, Conti, or another malware's command and control (C2).

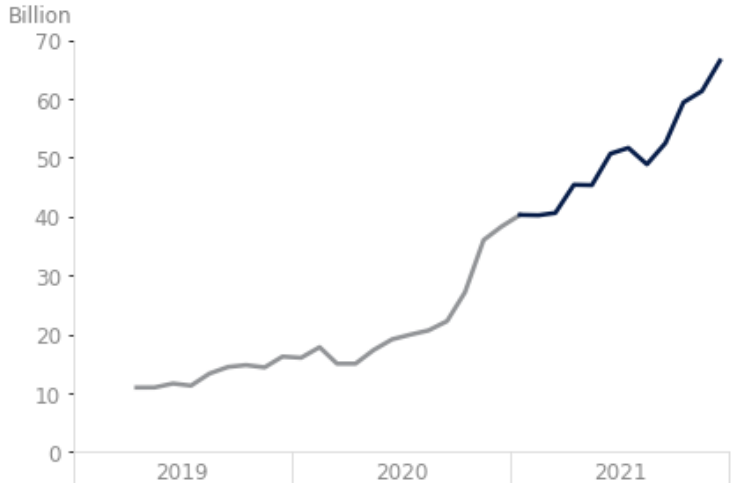


Figure 7 DNS Queries Resolved

FluBot

FluBot is malware that infects Android phones and devices. It is installed when a victim receives a text message asking them to install a tracking app due to a 'missed package delivery.' As the NCSC guidance points out, the app is in fact spyware that steals passwords and other sensitive data. It will access contact details and send out additional text messages, further spreading the problem. The research team at Nominet (our delivery partner for this service) analysed queries to known FluBot domains from 1st May to 31st December. All queries were blocked. The diagram below shows the number of unique domains blocked per week across the reporting period.

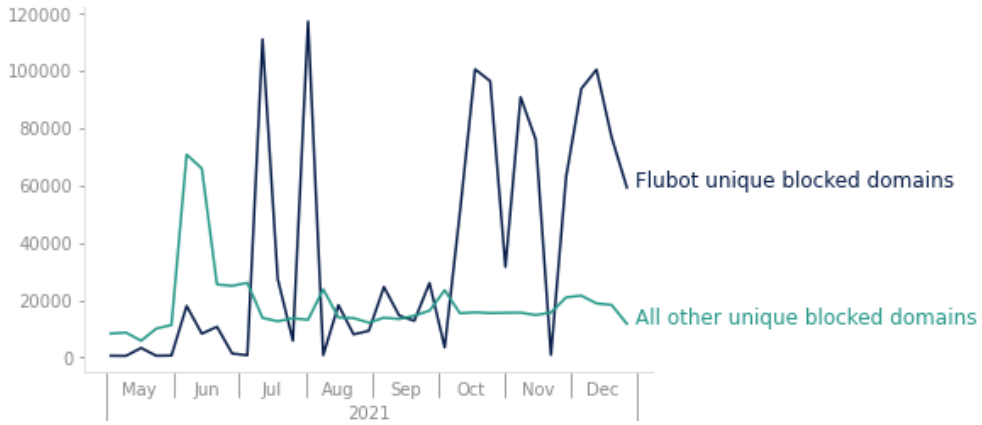


Figure 8 'FluBot unique' and 'all other unique' blocked domains for 2021

Early Warning

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

Early Warning is a free NCSC service designed to 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, 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 points of contact.

Key findings from the Early Warning service

The Early Warning customer base grew from approximately 2,000 signed up organisations to 4,750 over the year, following the 2021 CyberUK launch.

- The service sent out 92,260 notifications to 4,610 organisations. This covered 36,027,426 events of which 7,496,610 events were about potentially malicious activity that the customer would have needed to fix (such as malware infections or other indications of a system having been hacked). This is around 20,000 potentially malicious events per day.
- 28,528,582 were about potential misconfigurations, including 3,126,220 notifications of Remote Desktop Protocol (RDP) open to the internet, which is a common vector for ransomware actors to use.

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 common and 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 small-to-medium enterprises, the service has also seen strong take-up amongst large organisations and cyber security professionals.

Key findings from Exercise in a Box

In 2021, we reached a milestone with EiaB with over 10,000 users worldwide and have now, at the end of December, reached over 13,000 users across the world, a circa 50% increase over the start of the year boosted by the social media campaigns we ran as we added exercises to the tool. We saw increases in our public sector audience by around 49%, SMEs by 45%, large businesses by around 84% and cyber security professionals by around 63% over the December 2020 numbers.