SEARCHLIGHT CYBER

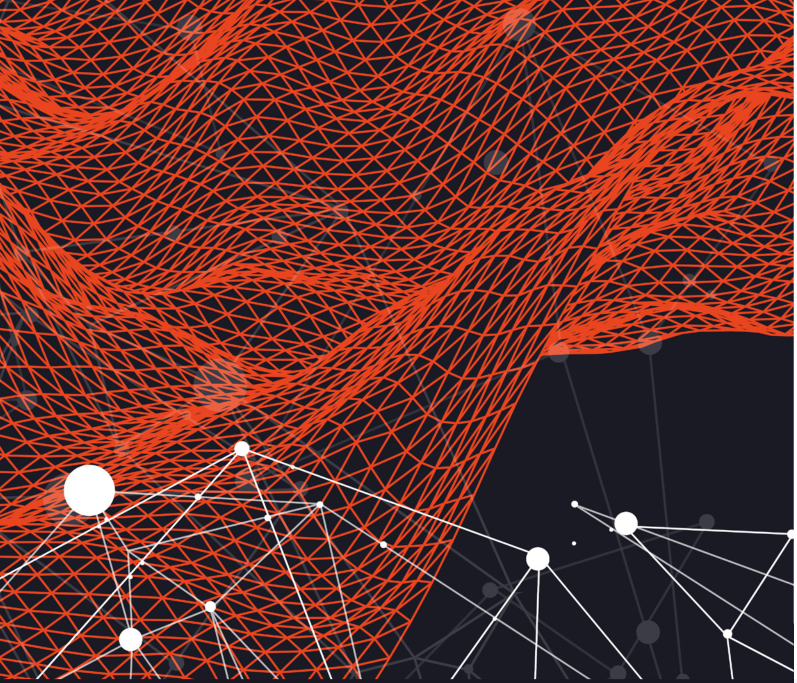
THE UK FROM A CYBERCRIMINAL'S PERSPECTIVE

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown
Commercial
Service
Supplier



SEARCHLIGHT CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM CYBER ESSENTIALS AICPA SOC Crown Commercial Service Supplier

CONTENTS

INTRODUCTION

What motivates cybercriminals to target the UK?

The vast majority of cybercrime is financially motivated, which makes countries with high-income economies such as the UK a target for threat actors. Quite simply, hackers recognize that they are more likely to make more money from targeting both organizations and individuals that have a higher net-worth.

Of course, there are other factors that threat actors consider when deciding to target one country over another. Language is another major consideration and also plays to the UK's disadvantage, as English is the default language of most computer systems. This means that most threat actors have some level of English proficiency, making UK-based organizations an attractive target as it is much easier for cybercriminals to navigate through networks where the system language and structure is set to English. It is also much easier for attackers to undertake social engineering attacks - like phishing - in a language they speak.

Geopolitics is another consideration. This report includes the activity of hacktivists, cybercriminals that are politically motivated to target the UK. However, even for financially-motivated hackers, geopolitics has an impact on targeting as cybercriminals are less likely to be arrested for targeting organizations in "unfriendly" nations. Many of the most active cybercriminal gangs targeting the UK are based in Russia or Russia-affiliated nations. Their cybercrimes may not be explicitly state-backed but the hackers are aware that the government largely turns a blind eye to the targeting of UK-based organizations and there is virtually no chance that they will ever be extradited to face time in a UK prison.

All of these factors combined means that the UK faces a high-volume of attacks from a diverse range of adversaries. In this report, we aim to provide an overview of the types of threat we observe against UK entities on the dark web - the part of the internet where cybercriminals routinely conduct their reconnaissance and plan their attacks.

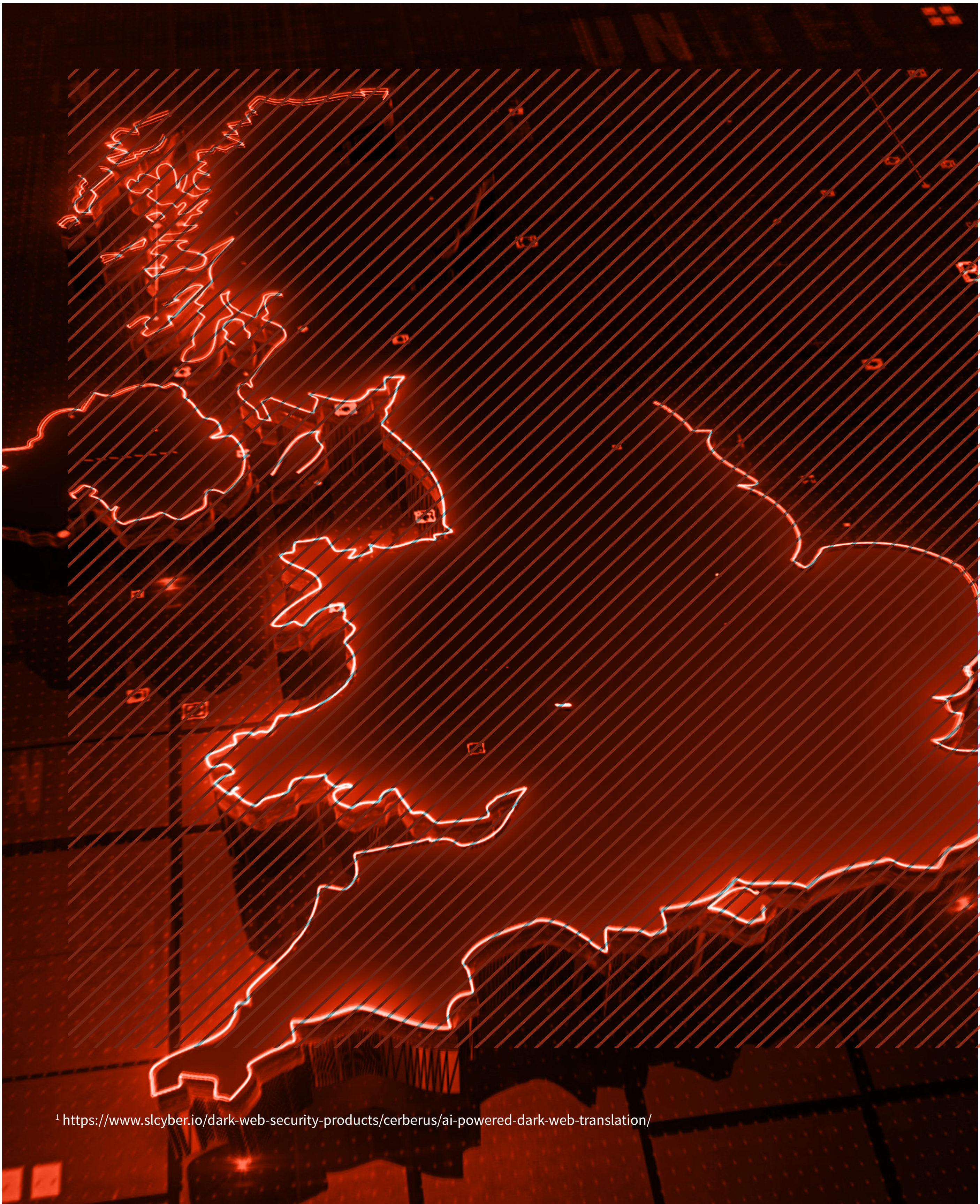
Monitoring the dark web and gathering intelligence from its hidden forums, sites, and marketplaces provides unique insights into the "cybercriminal perspective". This is a broad overview on the country level but demonstrates how interrogating dark web data can give security teams a better understanding of the threats they are facing.

LUKE DONOVAN

Head of Threat Intelligence
Searchlight Cyber

METHODOLOGY

The intelligence in this report was gathered from 2023 using our dark web investigation platform. Text from the dark web has been reformatted for readability. In some cases, data has been redacted for security purposes. Unless otherwise stated, the text is verbatim for how it appears on the dark web. We use our own proprietary translation technology[1] to convert text into English.



[1] https://www.slcyber.io/dark-web-security-products/cerberus/ai-powered-dark-web-translation/

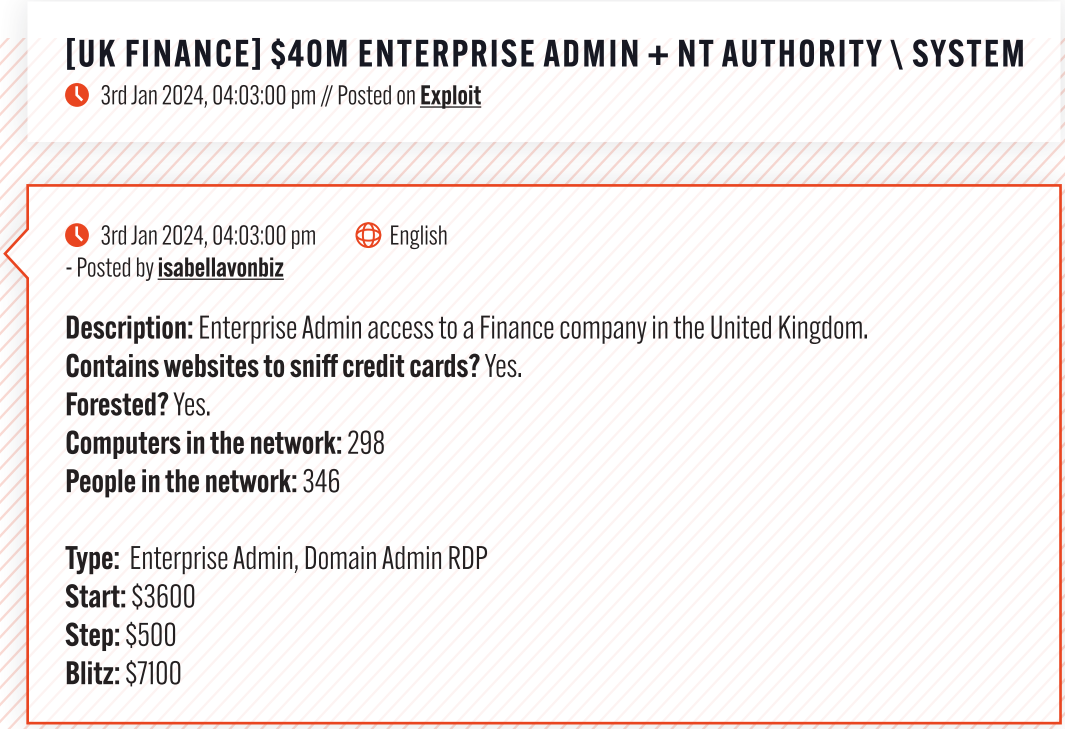
CYBERCRIMINALS TARGETING THE UK

INITIAL ACCESS BROKERS

Initial Access Brokers are threat actors that specialize in obtaining a foothold in a victim's system by leveraging a number of methods - including stealer logs, operating malware, exploiting vulnerabilities, or engaging in social engineering attacks. Once obtained, the Brokers sell the access to more specialized hackers - such as ransomware operators or database vendors - enabling them to execute their attacks.

The sales process - often in the form of an auction - typically takes place on cybercrime forums. According to our information, more than 105 Initial Access Broker advertisements about UK organizations were posted on the Exploit cybercrime forum alone in 2023. Exploit[2], XXS[3], BreachForums[4], Cracked[5], and Ramp[6] are some of the most popular hacking forums for Initial Access Broker posts and - between them - there were more than 300 listed UK organizations last year.

Figure 1 provides an example of an Initial Access Broker from Exploit: a threat actor operating under the alias isabellavonbiz auctioning access with domain administrator level privileges to a UK-based enterprise from the finance industry. The actor claimed that the access was maintained via a compromised Remote Desktop Protocol (RDP) account and would allow the buyer to engage in "payment card sniffing", a process for stealing card data. The Broker has set the starting price for the auction at $3,600 and indicated that bids should increase at a "Step" price of $500. They also establish an upper limit "Blitz" price of $7,100, which would allow a particularly interested hacker to buy the access outright.



[UK FINANCE] $40M ENTERPRISE ADMIN + NT AUTHORITY \ SYSTEM

3rd Jan 2024, 04:03:00 pm // Posted on Exploit

3rd Jan 2024, 04:03:00 pm English
- Posted by isabellavonbiz

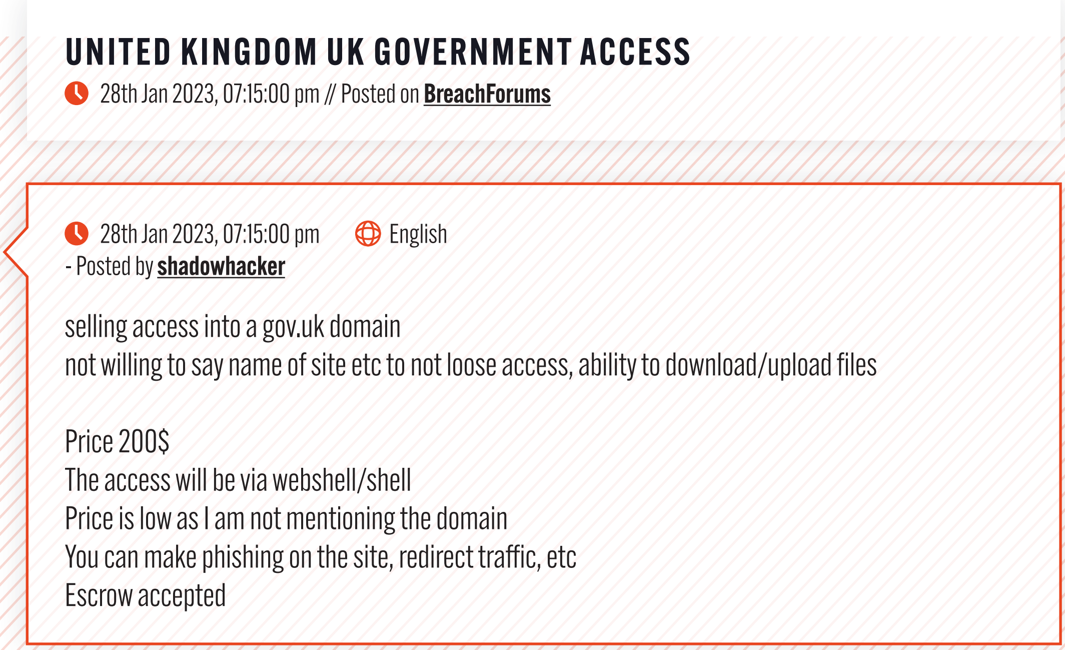
Description: Enterprise Admin access to a Finance company in the United Kingdom.
Contains websites to sniff credit cards? Yes.
Forested? Yes.
Computers in the network: 298
People in the network: 346

Type: Enterprise Admin, Domain Admin RDP
Start: $3600
Step: $500
Blitz: $7100

Figure 1: *An Initial Access Broker advertises a compromise in a UK finance company at the starting price of $3,600.*

Figure 2 shows an Initial Access Broker - shadowhacker - offering to sell access to the domain of a UK-based government institution on the hacking forum, BreachForums. The actor claimed the access was established via a web shell and suggested that it could be used to conduct phishing attacks, redirect traffic, download, and upload files.

Rather than selling their access via an auction, shadowhacker provides one price ($200) and offers to sell the access via escrow. Most cybercrime forums have an escrow service, where a third party (sometimes the forum admin) holds the money from the buyer while the access is certified as legitimate. This service comes at a cost but ensures that the buyer actually receives the access they have paid for. It is also a way for Initial Access Brokers to demonstrate their "legitimacy", which is important in the case of this sale as the Broker refuses to name the site they claim to have gained access to.



UNITED KINGDOM UK GOVERNMENT ACCESS

28th Jan 2023, 07:15:00 pm // Posted on **BreachForums**

28th Jan 2023, 07:15:00 pm English
- Posted by **shadowhacker**

selling access into a gov.uk domain
not willing to say name of site etc to not loose access, ability to download/upload files

Price 200$
The access will be via webshell/shell
Price is low as I am not mentioning the domain
You can make phishing on the site, redirect traffic, etc
Escrow accepted

Figure 2: *An Initial Access Broker advertises a web shell in an unnamed gov.uk domain.*

[2] https://www.slcyber.io/dark-web/exploit/
[3] https://www.slcyber.io/dark-web/xss/
[4] https://www.slcyber.io/dark-web/breachforums/
[5] https://www.slcyber.io/dark-web/cracked/
[6] https://www.slcyber.io/dark-web/ramp/

RANSOMWARE

Ransomware operators also have a preference for UK-based entities. According to our data, UK organizations were listed as victims of ransomware groups at least 330 times in 2023, second only to organizations from the United States.

It is worth noting that these are only the organizations that the ransomware groups (which we track) have publicly named, and this figure is almost certainly an underestimate of the actual number of UK enterprises that were impacted by ransomware last year. For example, some ransomware groups do not have dark web leak sites that they use to shame their victims, while others will negotiate with victims privately and only list victims that refuse to pay the ransom.

Attackers seek to target high-revenue organizations or entities where ransomware will have a high-impact, such as critical infrastructure, meaning that there is more pressure for the organizations to pay out. Some examples of UK entities directly impacted by ransomware attacks last year include the Royal Mail, and (indirectly, through third party attacks) the Ministry of Defence and the Greater Manchester Police. There were occasions when ransomware operators launched attacks against the National Health Service (NHS), exfiltrating patient data. According to our observations (**Figure 3**), the highest number of UK victims are active in the Commercial & Professional Services industries.

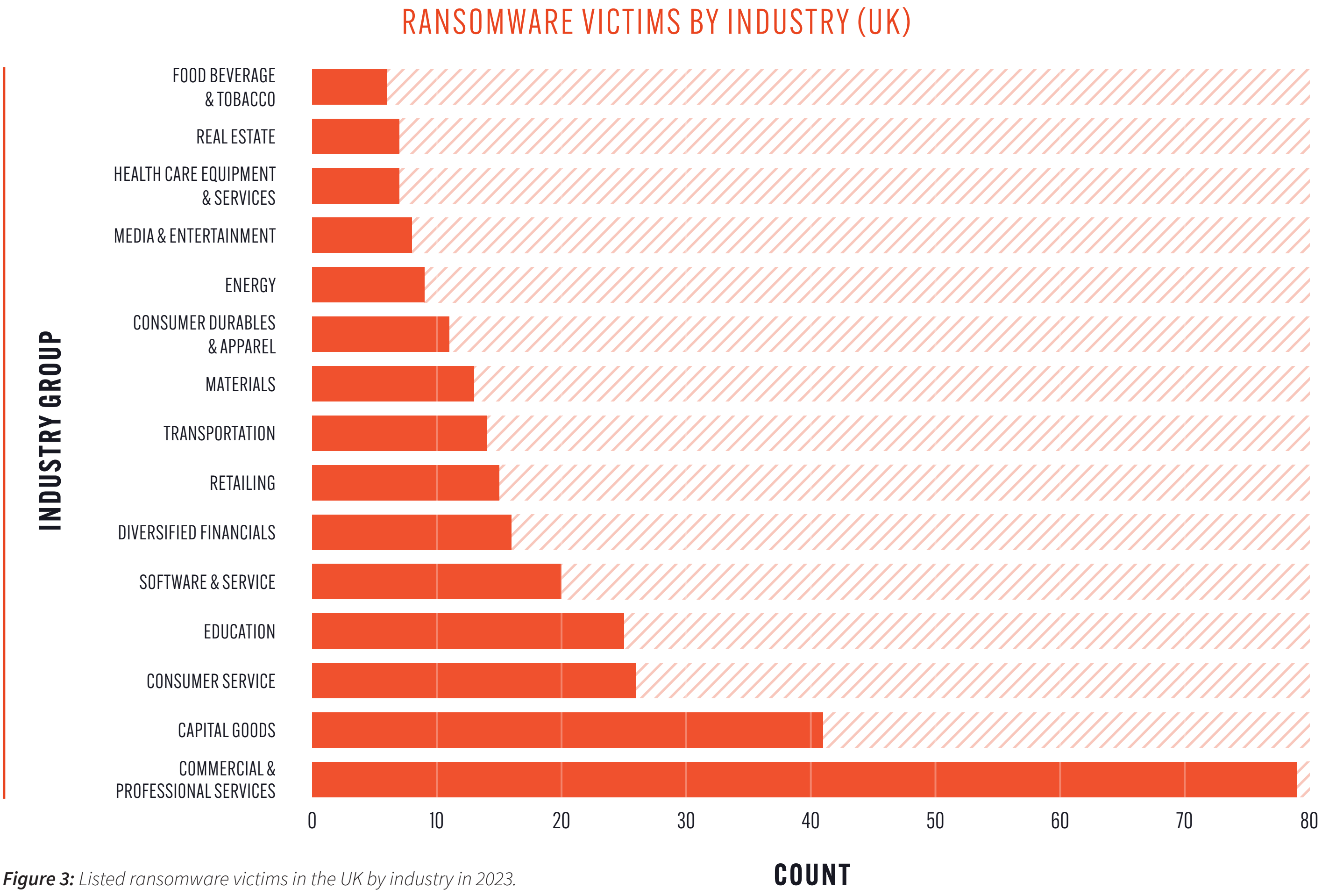


Figure 3: *Listed ransomware victims in the UK by industry in 2023.*

It is worth noting that firms in the UK are targeted constantly - we typically see between two and three new victims per week. However, there were spikes of up to nine UK victims being claimed by ransomware gangs (see **Figure 4**).

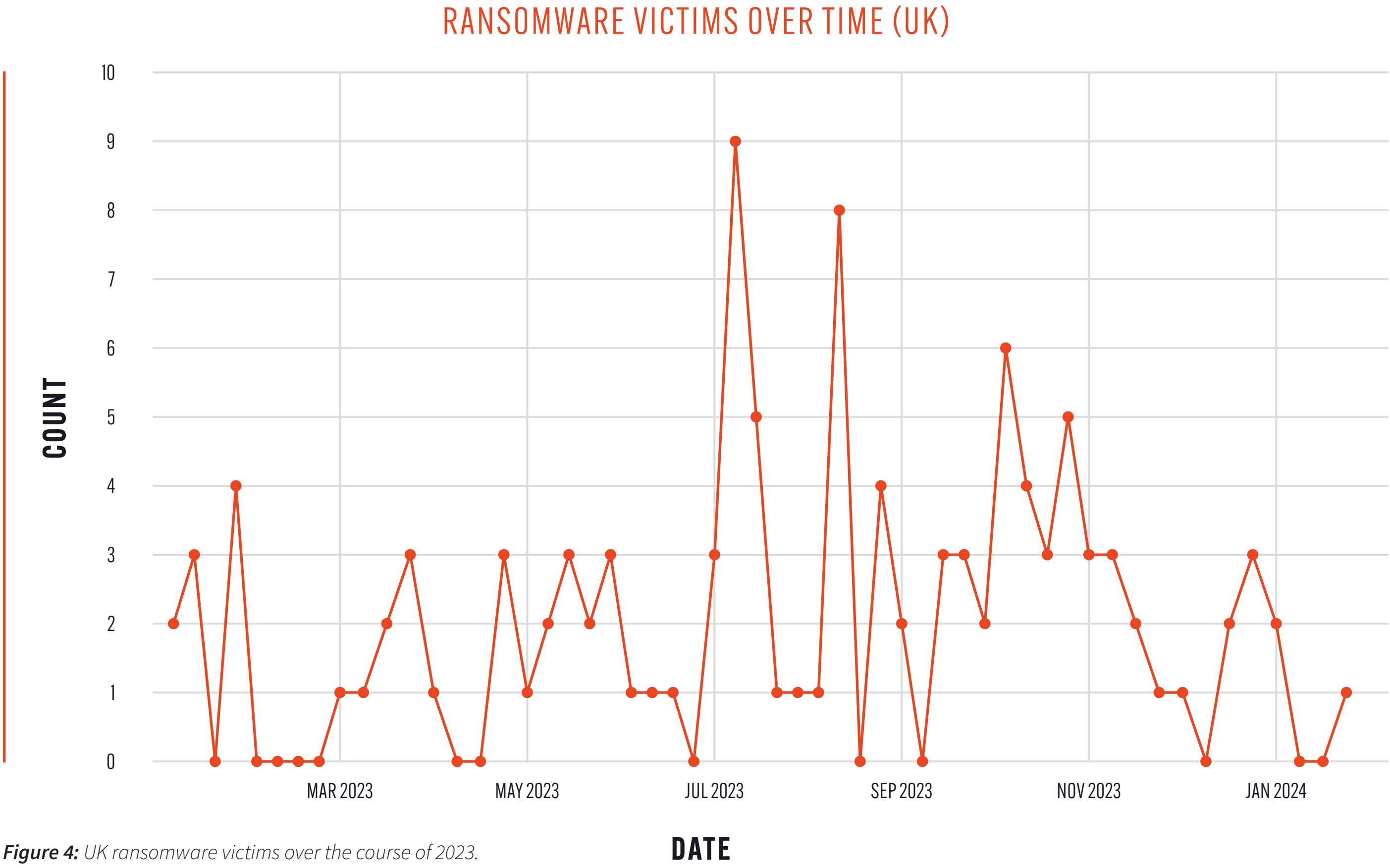
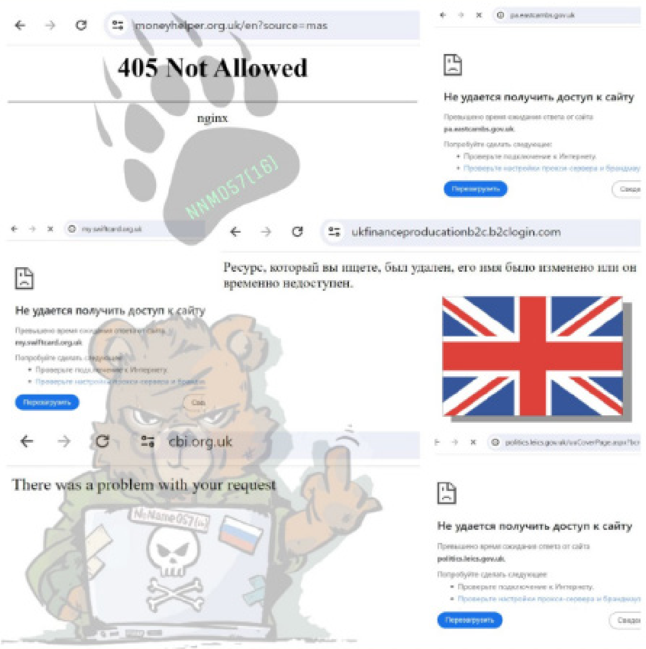


Figure 4: *UK ransomware victims over the course of 2023.*

HACKTIVISM


moneyhelper.org.uk/en?source=mas
NNM057(16)
ukfinanceproducationb2c.b2clogin.com
cbi.org.uk
NoName057(16)
Перезагрузить

405 Not Allowed

nginx

Не удается получить доступ к сайту

Ресурс, который вы ищете, был удален, его имя было изменено или он временно недоступен.

There was a problem with your request

British Prime Minister Rishi Sunak and Ukrainian President Volodymyr Zelenskyy have signed an agreement on security cooperation. The signing of the doument took place in Kyiv, the Ukrainian head shared the relevant footage in his Telegram channel. Also Britain will send 20 thousand military personnel to NATO exercises to flight Russia

Well while Britain is sending soldiers to the exercises, we are sending our DDoS missiles 👿 to this country:

❌ **Confederation of British Industry**
(closed on geo) check-host.net/check-report/14a819fbk391

❌ **Swift card authorization**
check-host.net/check-report/14a81bbfkd07

❌ **Authorization UK Finance - Merchant Organization**
check-host.net/check-report/14a81d20kfec

❌ **Money Advice Service financial planning tips & guides**
check-host.net/check-report/14a81e55k1c

❌ **Leicestershire County Council**
check-host.net/check-report/14a82247kf88

❌ **East Cambridgeshire District Council**
(closed on geo) check-host.net/check-report/14a82390ka11

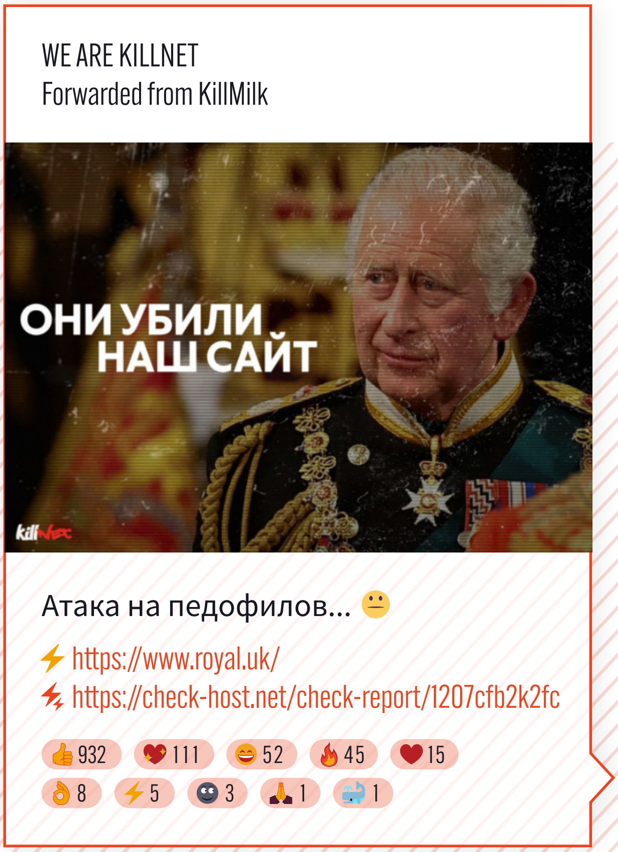
Figure 5: *A hacktivist group called NoName057(16) publicizes its attacks on UK entities on its Telegram channel.*

Unlike ransomware groups and Initial Access Brokers, hacktivists do not engage in cyberattacks for financial gain. Hacktivists are motivated by proving a point or making a statement and their victims are generally selected based on an opposing ideological, (geo)political, or moral view to the hackers.

The UK has been targeted by hacktivists in the context of the Russia-Ukraine war, with attacks coming from Russia-based hackers who do not agree with the UK's military and financial aid for Ukraine. **Figure 5**, for the example, shows a group that has claimed to impact a number of UK entities, following the implementation of a security cooperation agreement between the UK and Ukraine.

As the hackers in **Figure 5** allude to, the most common technique deployed by hacktivists is distributed denial-of-service (DDoS) attacks, which look to temporarily disrupt services by flooding them with requests, although there are also instances where threat actors have exfiltrated and leaked sensitive data. Governmental institutions, schools, financial services, and critical infrastructure are the most common targets of hacktivists.

Figures 6 and 7 show two more examples of posts from Russian-affiliated hacktivists groups - KillNet and Team_R70. KillNet has become an especially infamous group through the Russia-Ukraine war, using its Telegram channel to publicize attacks against Ukraine and its allies, as well as to spread Russian propaganda and misinformation.



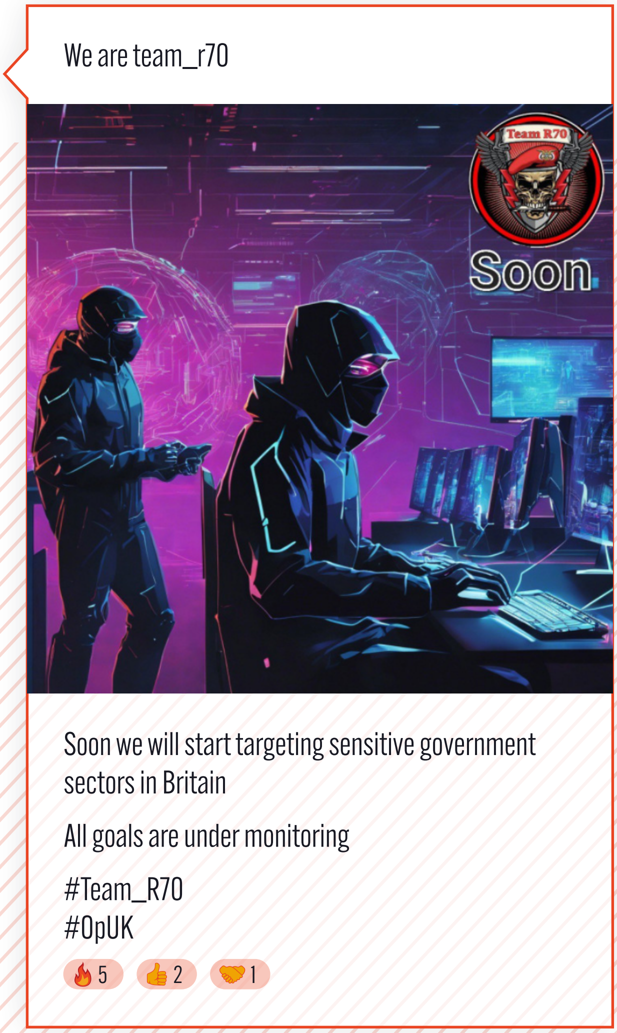
WE ARE KILLNET
Forwarded from KillMilk

Атака на педофилов... 😐

⚡ https://www.royal.uk/
⚡ https://check-host.net/check-report/1207cfb2k2fc

👍 932 💔 111 😄 52 🔥 45 ❤ 15
👌 8 ⚡ 5 🌚 3 🙏 1 🐳 1

***Figure 6:** The infamous hacktivist group KillNet claims an attack on royal.uk, the website of the UK royal family. The text in the photo reads: "Our website was taken down".*



We are team_r70

Soon we will start targeting sensitive government sectors in Britain

All goals are under monitoring

#Team_R70
#OpUK

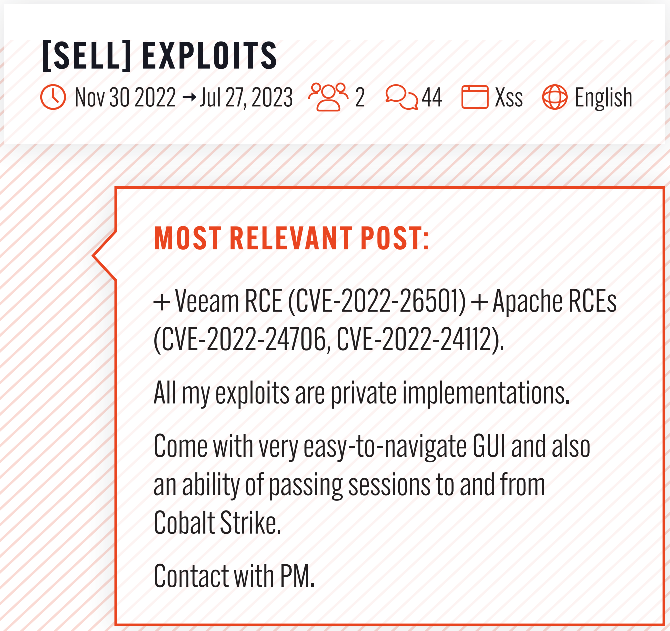
🔥 5 👍 2 🤝 1

***Figure 7:** Team_R70 vows to target government organizations in Britain, under the hashtag #OpUk.*

COMMON VULNERABILITIES AND EXPOSURES (CVE)

Improper setup or the use of outdated software can allow threat actors to exploit vulnerable systems to conduct their attacks. For example, some of the Initial Access Brokers already discussed in this report actively scan for vulnerabilities to exploit as their main attack vector. Typically, most vulnerabilities are found by the software developers before they are weaponised in the wild - with "zero day" vulnerability attacks being relatively rare. However, applying patches to vulnerable software is a time consuming and resource-intensive process, which means that organizations are often caught out by known vulnerabilities that simply have not been addressed in time.

A quick search using Shodan revealed that at least 110 systems in the UK are vulnerable to CVE-2022-24706, an Apache CouchDB vulnerability that allows threat actors to obtain unauthorized admin privileges. Notably, remote code execution is possible by exploiting this vulnerability. According to our data sets, several actors are discussing the vulnerability on dark web forums, including Chinese-speaking actors. Moreover, some actors are also selling exploits to aid exploitation of such vulnerabilities (see **Figure 8**).



[SELL] EXPLOITS

Nov 30 2022 → Jul 27, 2023 2 44 Xss English

MOST RELEVANT POST:

+ Veeam RCE (CVE-2022-26501) + Apache RCEs (CVE-2022-24706, CVE-2022-24112).

All my exploits are private implementations.

Come with very easy-to-navigate GUI and also an ability of passing sessions to and from Cobalt Strike.

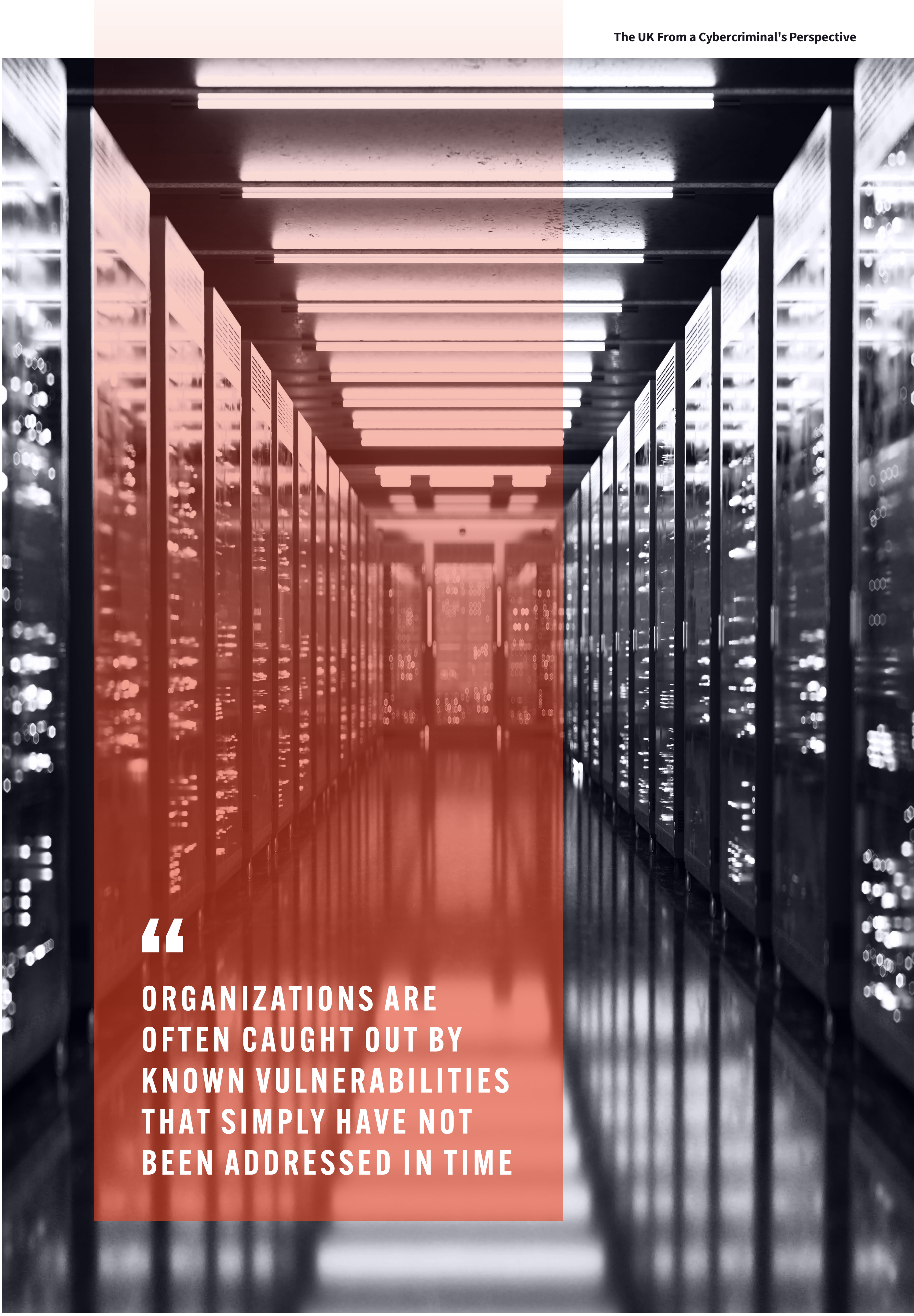
Contact with PM.

***Figure 8:** A cybercriminal advertises exploits for two CVEs on the popular hacking forum XSS.*

Another similar example is CVE-2022-36804, a command injection vulnerability found in Atlassian Bitbucket Server. We have observed vulnerable systems based in the UK, as well as threat actors selling exploits for it on dark web forums. However, on this occasion, methods of exploitation have been widely discussed even on open sources, allowing any actor to use the knowledge with malicious intent.

A vulnerability enabling HTTP Request smuggling attacks on Apache HTTP Server has been discussed on open sources, including on Github, where the user dhmosfunk shared[7] a comprehensive proof-of-concept. According to our observations, there were more than 190,000 vulnerable systems operating in the UK. By exploiting this vulnerability (CVE-2023-25690) an attacker could bypass access controls.[8]

[7] https://github.com/dhmosfunk/CVE-2023-25690-POC
[8] https://httpd.apache.org/security/vulnerabilities_24.html



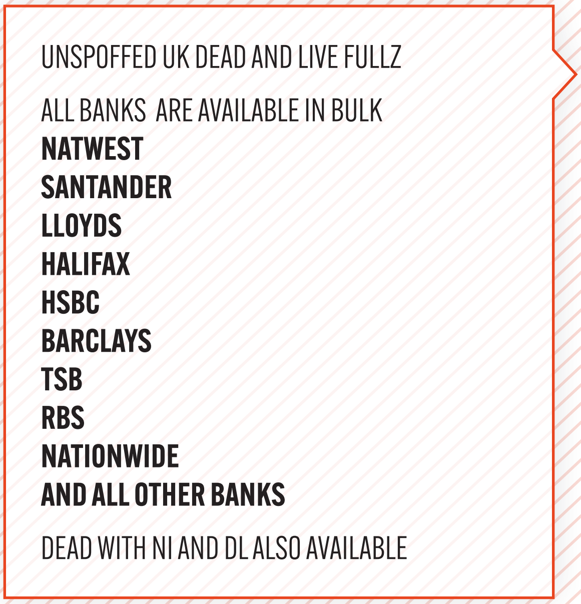
“

ORGANIZATIONS ARE OFTEN CAUGHT OUT BY KNOWN VULNERABILITIES THAT SIMPLY HAVE NOT BEEN ADDRESSED IN TIME

FRAUD AND STOLEN GOODS

Beyond traditional “cybercrime” the dark web is also a hub of criminal activity including fraud, forgery, and the trade of stolen goods - which also impacts UK businesses and individuals.

Often, these activities are focused on “digital goods”. For example, on Telegram we routinely observe the sale of “fullz”, a slang term that refers to the sale of an individual's “full” financial information, which is typically used to conduct fraud (see **Figure 9**).



UNSPOFFED UK DEAD AND LIVE FULLZ

ALL BANKS ARE AVAILABLE IN BULK
NATWEST
SANTANDER
LLOYDS
HALIFAX
HSBC
BARCLAYS
TSB
RBS
NATIONWIDE
AND ALL OTHER BANKS

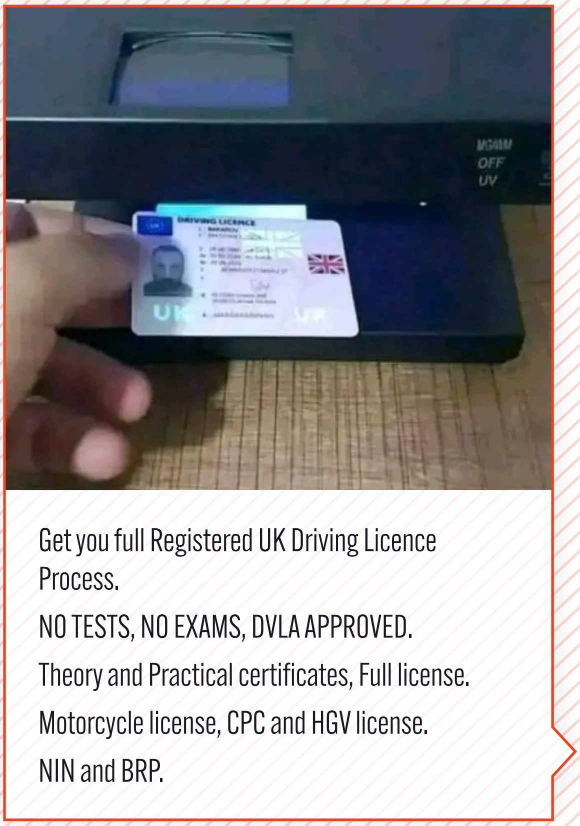
DEAD WITH NI AND DL ALSO AVAILABLE

Figure 9: *A vendor on Telegram offers “fullz” from the UK, in relation to several banks.*

This information can come from a number of sources:

- **SOCIAL ENGINEERING ATTACKS** where individuals are tricked into handing over their data to the attacker, for example through a fake website, on the phone, or via email.
- **MALICIOUS INSIDERS** where individuals who have access to sensitive information - for example the staff of a bank - sell data onto cybercriminals.
- **INFORMATION-STEALER LOGS** a type of malware that sits on a device and passes back sensitive information - such as passwords and usernames - to the attacker.

We have even observed some sets of fullz for sale with scanned copies of documents such as driving licenses or passports. Other vendors offer forged documents, including driving licenses, and promise their products would pass any verification from the Driver and Vehicle Licensing Agency (DVLA) or other relevant authorities (see **Figure 10**).



Get you full Registered UK Driving Licence Process.

NO TESTS, NO EXAMS, DVLA APPROVED.

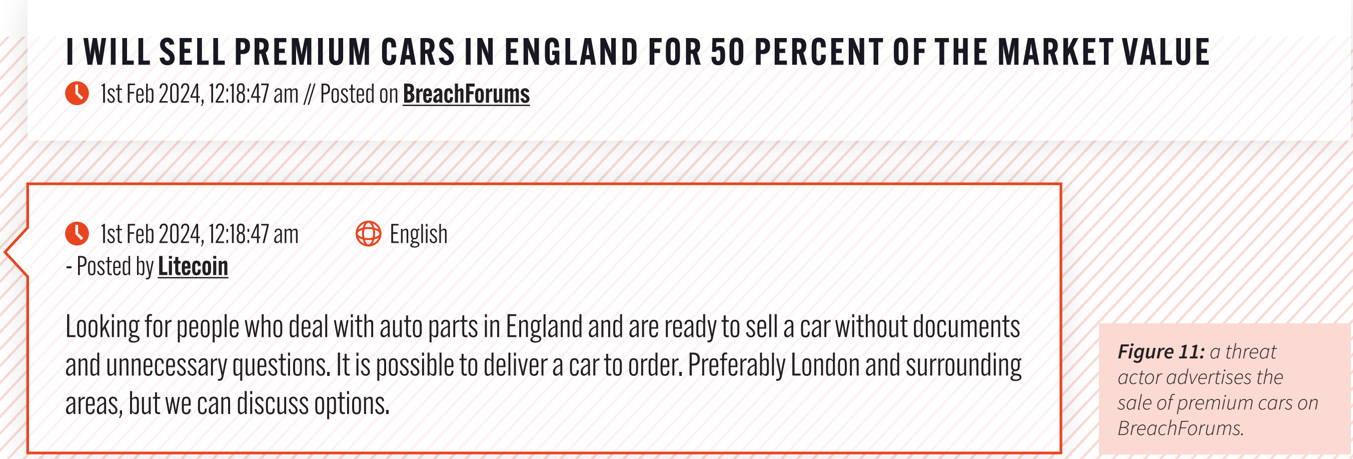
Theory and Practical certificates, Full license.

Motorcycle license, CPC and HGV license.

NIN and BRP.

Figure 10: *A Telegram user advertises the sale of UK driving licenses.*

Recently we have even observed underground forums being used by criminals to sell premium cars in the UK - likely stolen - to buyers looking to pay half of their normal price and are happy to use them without documents. The seller in **Figure 11** even offered to provide cars specifically ordered by buyers, as long as they promise not to ask “unnecessary questions”. This particular seller appeared to serve the London area, but expressed willingness to go beyond the city limits.



I WILL SELL PREMIUM CARS IN ENGLAND FOR 50 PERCENT OF THE MARKET VALUE

1st Feb 2024, 12:18:47 am // Posted on **BreachForums**

1st Feb 2024, 12:18:47 am English
- Posted by **Litecoin**

Looking for people who deal with auto parts in England and are ready to sell a car without documents and unnecessary questions. It is possible to deliver a car to order. Preferably London and surrounding areas, but we can discuss options.

***Figure 11:** a threat actor advertises the sale of premium cars on BreachForums.*

> “
>
> BEYOND TRADITIONAL “CYBERCRIME” THE DARK WEB IS ALSO A HUB OF CRIMINAL ACTIVITY INCLUDING FRAUD, FORGERY, AND THE TRADE OF STOLEN GOODS

CONCLUSION

Threat actors will make an effort to conduct a cyberattack if they consider the rewards - whether it is money, fame, or self-fulfillment - worth the hassle. Unfortunately for the UK, there are lots of incentives for cybercriminals to target organizations in this region.

As this report demonstrates, the methods cybercriminals use to execute their attacks vary greatly - and cybercriminals will continue to come up with new strategies, tools, and techniques to attack UK businesses. This means that, from the perspective of a UK organization, there will never be one simple solution to stop the cybercrime they face. Instead, security teams need to focus on monitoring the latest attack techniques, determine the most likely ways they are going to be attacked based on the intelligence they have, and continuously adapt their security measures as the cybercriminal threat changes.

Organizations should engage in intelligence operations in order to identify any indication or warning of a potential attack being planned. This action will also enable the identification of threat actors, their motivations and intentions, an understanding of their capability, and lastly any opportunities which could be exploited by them.

Other tips to help protect your assets:

➤ EDUCATE CUSTOMERS AND EMPLOYEES

Awareness about common threats is vital, employees are often viewed as a weak link even in a mature cyber security program and sometimes are exploited by ransomware operators,[9] while customers should be able to detect a fraudulent call during a vishing attempt.

➤ ADOPT A PROACTIVE APPROACH TO VULNERABILITY MANAGEMENT

Those responsible for network and infrastructure security should stay up to date with the latest CVEs and continuously update[10] and monitor their systems.

➤ MONITOR THE DARK WEB FOR PRE-ATTACK INTELLIGENCE

By keeping a close eye on the newest methods discussed by threat actors on the dark web, security teams can gain vital time to secure systems before hackers get a chance to put their endeavors into practice.

[9] https://www.darkreading.com/cybersecurity-operations/identity-alone-wont-save-us-tsa-paradigm-mgm-hack

[10] https://news.sophos.com/en-us/2024/04/03/unpatched-vulnerabilities-the-most-brutal-ransomware-attack-vector/

GATHERING DARK WEB INTELLIGENCE

Criminals use the dark web to plan their attacks, share tactics, and buy the resources they need because they believe its anonymity will stop them from being identified. However, this makes the dark web an invaluable source of intelligence on the criminal ecosystem - and provides security teams with a unique insight into the cybercriminal perspective on their business.

Gathering intelligence from the dark web can help organizations to identify the cybercriminals that are targeting their geography, industry, or even their specific company - understand their tactics - and adjust their security strategy accordingly. This visibility into cybercriminal activity outside of the network gives organizations a rare opportunity to act before the threat actor has launched their attack, meaning that breaches can be completely avoided.

Governments, law enforcement agencies, and enterprises around the world use Searchlight Cyber's dark web investigation and monitoring tools in their fight against criminal activity on the dark web:

DARK WEB INVESTIGATION

DARK WEB SEARCH

Query more than 15 years of dark web data gathered from forums, marketplaces, hidden sites, cybercriminal communication channels, and more.

STEALTH BROWSER

Safely access dark web sites through a secure virtual browser to gather threat intelligence on cybercriminals directly from the source.

RANSOMWARE SEARCH AND INSIGHTS

Track and investigate the dark web activity of the most active ransomware groups through a continuously updated dashboard.

DARK WEB INVESTIGATION

ATTRIBUTE-BASED MONITORING

Continuously scan the dark web for attributes related to your organization - including domains, ports, IP addresses, and employee credentials.

DARK WEB TRAFFIC MONITORING

Monitor traffic to and from an organization's network and Tor, a reliable signal of malicious activity.

EXTERNAL ATTACK SURFACE MONITORING

Identify IP address and port vulnerabilities by using dark web exposure analysis to assess your footprint beyond your perimeter.

SEARCHLIGHT.
CYBER

VISIT **WWW.SLCYBER.IO** TO FIND
OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
200 Massachusetts
Avenue Northwest,
Washington, DC 20001
United States