SOCRadar®
Your Eyes Beyond

UK

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

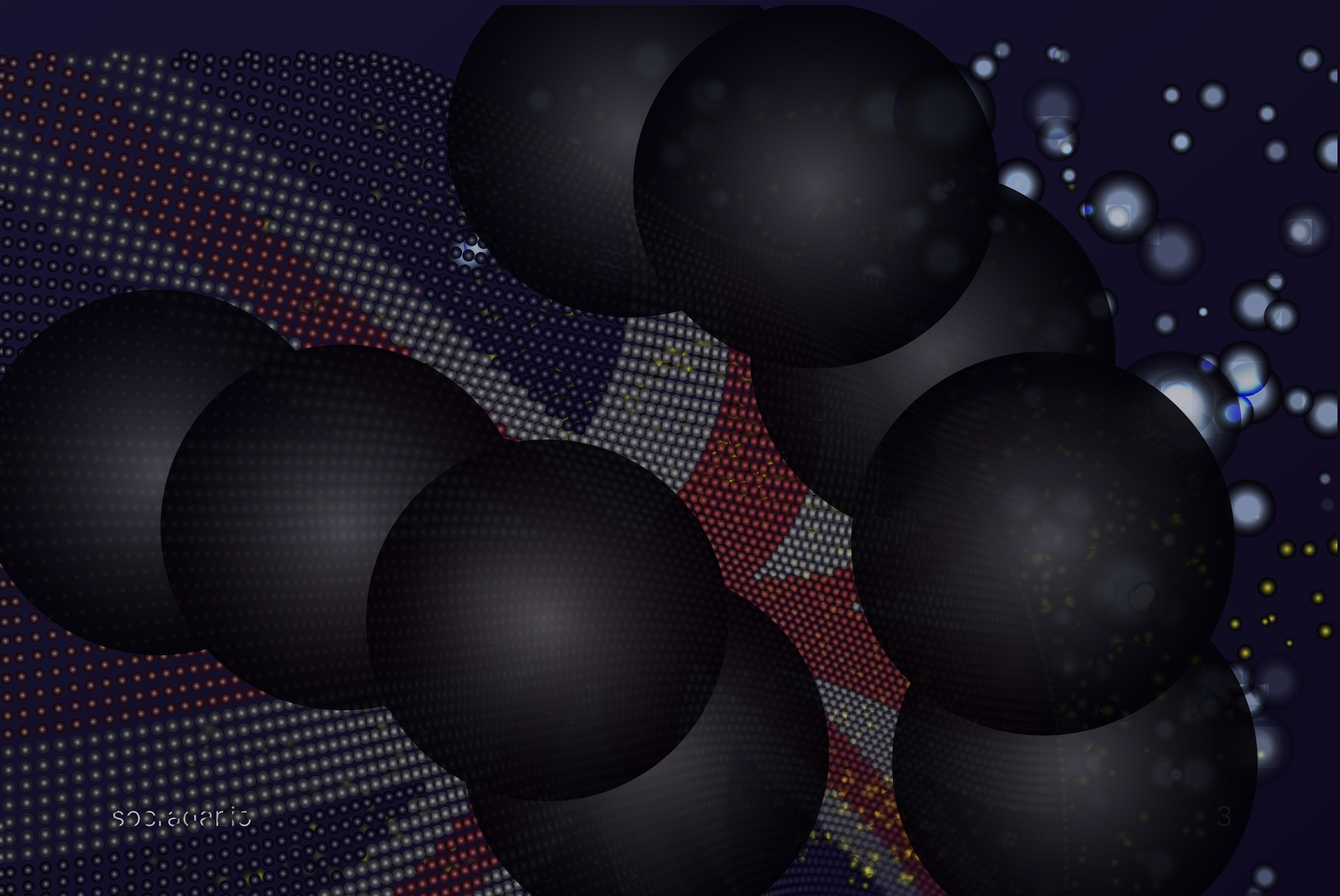
Table of Contents

Executive Summary

As one of the world's leading economies and a key player in global affairs, the United Kingdom holds a prominent position in innovation, finance, and industry.

However, alongside its economic prowess comes the ever-looming shadow of cyber threats, propelled by escalating global tensions and the evolving nature of digital warfare. The UK has witnessed a surge in sophisticated cyber operations as rival states exploit digital vulnerabilities to achieve their objectives.

Our report summarizes challenges originating from cyberspace, leveraging a combination of data sources and analysis techniques to provide insights into the evolving cyber threat landscape facing the United Kingdom.



Top Takeaways

Retail trade emerged as the most targeted industry in the UK during 2023, comprising 14,47% of threats from the dark web.

The second most targeted industry was Finance and Insurance, with 12,13% of the total dark web posts.

The predominant activity on the dark web in 2023 was the sale of various types of information, including leaks, accounting for 51,52% of illicit transactions.

The most significant share of this market was allocated by data and databases ranking first among different threat types on the dark web, representing 47,22% of all identified threats.

Political turmoil in another part of the world resulted in the resurgence of threat actors.

The hacking group Cyber Toufan has resurfaced, posing a cyber threat to the UK due to the Israel-Hamas conflict.

The primary ransomware target was the Manufacturing sector.

The manufacturing sector is the most impacted by ransomware attacks, accounting for 14,81% of all incidents.

Notorious ransomware groups are not leaving the throne to others.

The top ransomware groups targeting the UK were LockBit 3.0, Cl0p, and Black Basta.

The industry most targeted by phishing attacks was information services.

Organizations in the information services industry were the primary targets of phishing attempts, comprising 18,48% of all attacks. We believe this number is higher than that of other industries due to the extensive use of digital communication tools in the information services sector.

Stealer Logs reveals the vulnerabilities of thousands of accounts.

A significant number of passwords totaling 351,555 from the most frequently visited domains in the UK have been compromised and collected from Stealer Logs.

Attackers were determined to cut down the connections. This year, DDoS attacks lasted for 32 minutes on average.

In total, 115,193 Distributed Denial of Service (DDoS) attacks were recorded throughout the year.

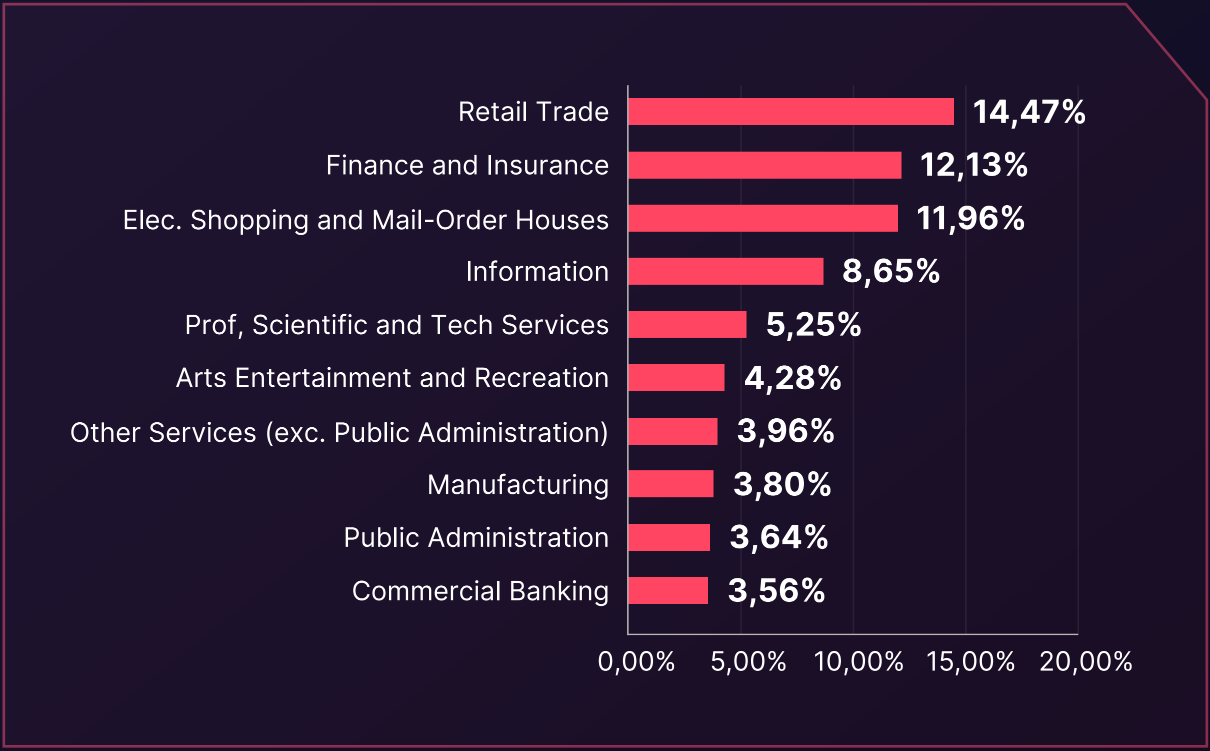
Dark Web Threats

Throughout the last year, SOCRadar's intelligence analysts meticulously tracked threat actors' activities within the dark web, documenting significant trends and actions targeting the United Kingdom. Notable efforts included the identification of tactics and the mapping of connections between threat actors and vulnerable sectors.

From the beginning of 2023 until the first quarter of 2024, 434 distinct threat actors shared 726 posts about their illicit activities targeting the United Kingdom, predominantly to sell or share the content they purportedly stole. This year's most targeted industry was Retail Trade, followed by Finance and Insurance, and in third place, there were Electronic Shopping and Mail-Order Houses.

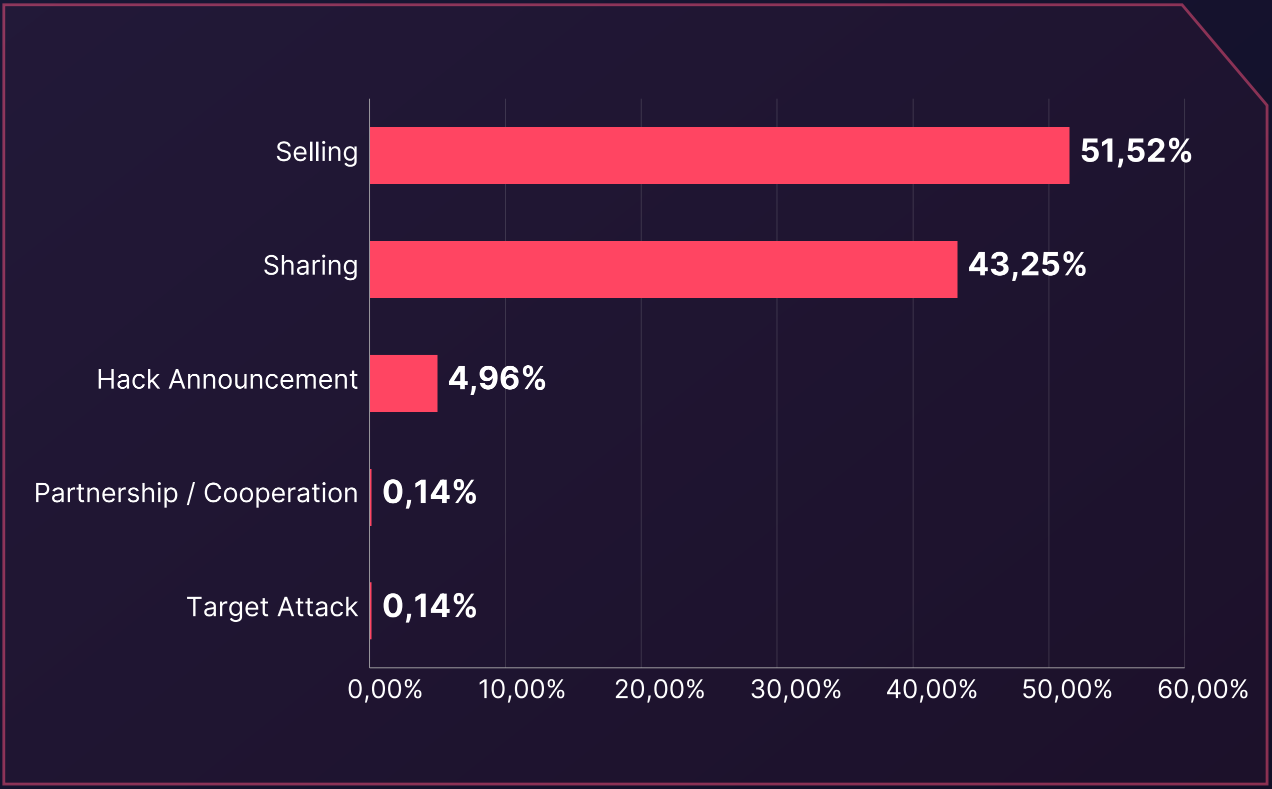
Closer Look into the Industries

Dark Web Threats- Distrubition by Industries



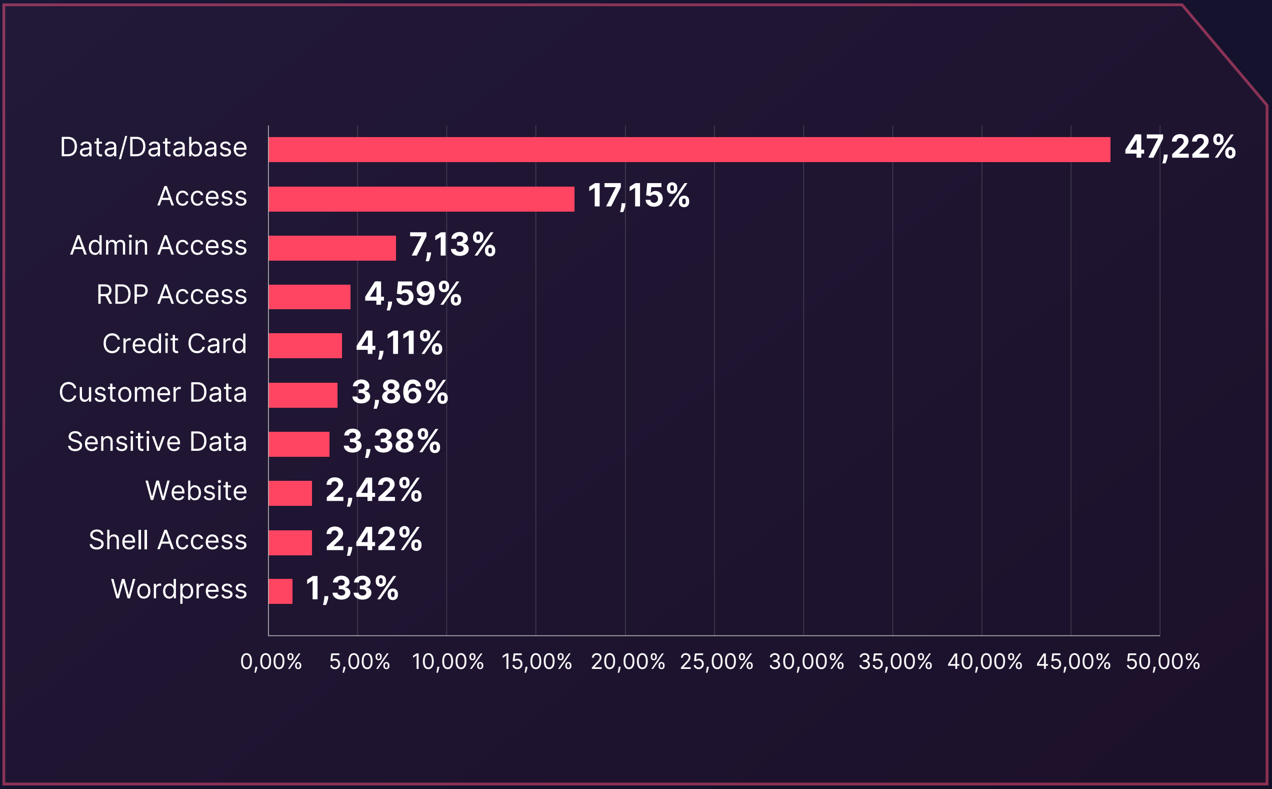
Exploring Threat Categories

Dark Web Threats- Distribution Threat Categories



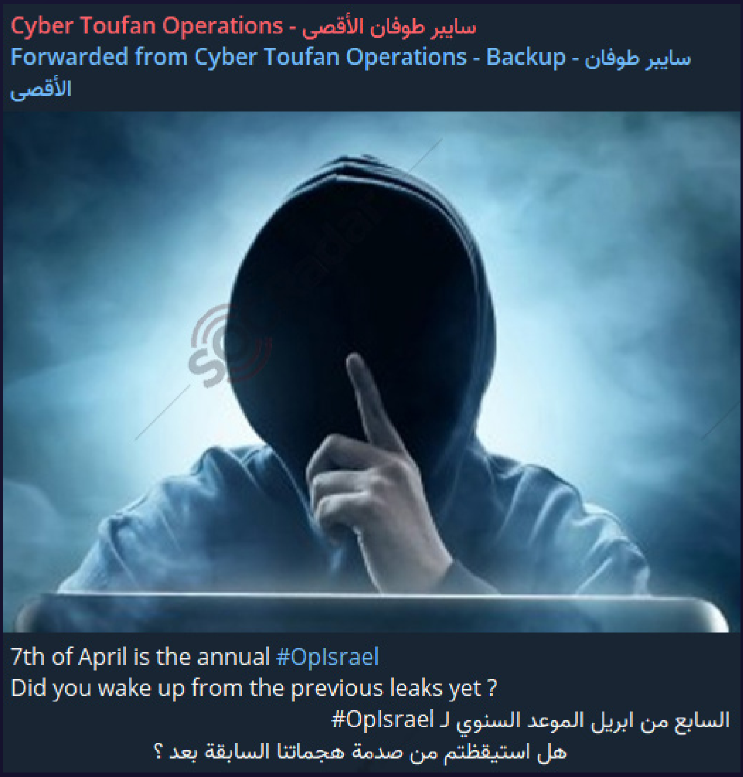
Top Threat Types

Dark Web Threats- Distibution by Threat Type



Recent Developments From the Dark Web

08 Apr
2024



Cyber Toufan Operations - سايبر طوفان الأقصى
Forwarded from Cyber Toufan Operations - Backup - سايبر طوفان الأقصى

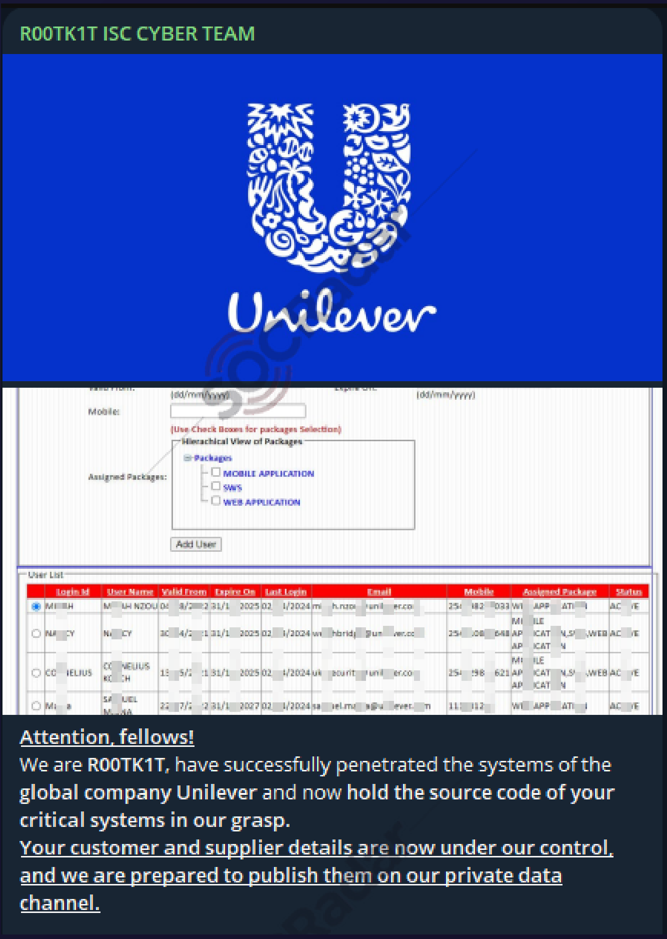
7th of April is the annual #OpIsrael
Did you wake up from the previous leaks yet ?
السابع من ابريل الموعد السنوي لـ #OpIsrael
هل استيقظتم من صدمة هجماتنا السابقة بعد ؟

Screenshot from Cyber Toufan's Telegram Channel

The hacking group Cyber Toufan has re-emerged, signaling its presence with DDoS attacks as part of #OpIsrael. A variety of cyber threats are present, with various groups employing tactics such as micro-DDoS attacks under the guise of the Toufan tag, targeting Israeli websites in alignment with #OpIsrael. Hacktivists explicitly designate countries like the UK as Israeli allies in their videos, making them targets. The array of attacks, spanning DDoS, defacement, and data leaks, presents a troubling landscape of cybersecurity challenges for the UK.

You can check our threat actor profile from here for more details.

02 Apr
2024



R00TK1T ISC CYBER TEAM

Valid From: (dd/mm/yyyy) Expire On: (dd/mm/yyyy)

Mobile:

(Use Check Boxes for packages Selection)

Assigned Packages:

Hierachical View of Packages

⊟ Packages
- ☐ MOBILE APPLICATION
- ☐ SWS
- ☐ WEB APPLICATION

Add User

User List

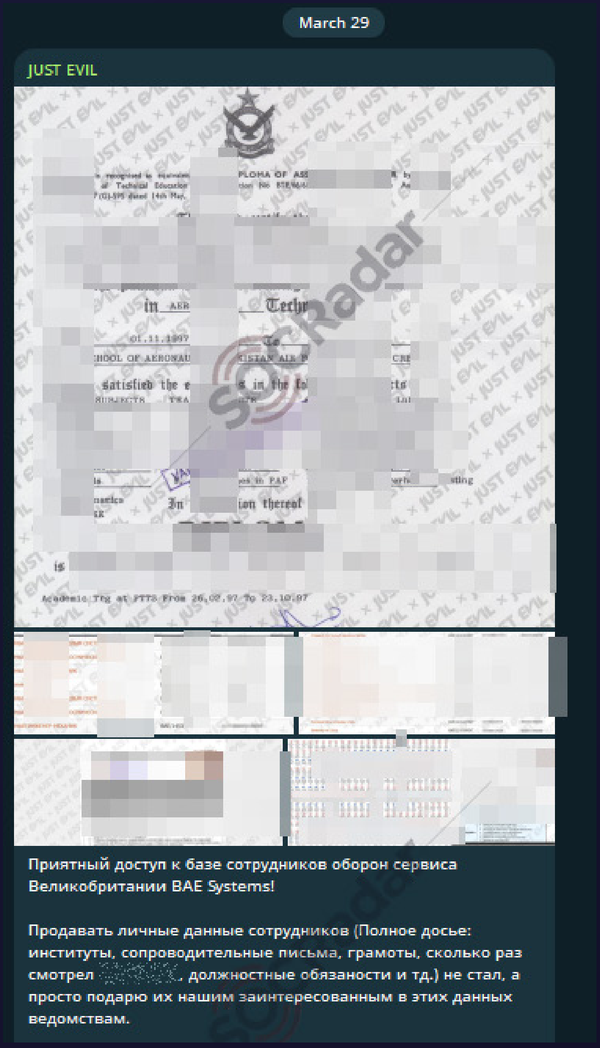
	Login Id	User Name	Valid From	Expire On	Last Login	Email	Mobile	Assigned Package	Status
●	MI[redacted]H	M[redacted]AH NZOU	0[redacted]2	31/1[redacted]2025	02[redacted]/2024	m[redacted]er.co	25[redacted]033	WE[redacted]	AC[redacted]E
○	NA[redacted]CY	N[redacted]CY	3[redacted]1	31/1[redacted]2025	02[redacted]/2024	w[redacted]er.co	25[redacted]648	MO[redacted]N	AC[redacted]E
○	CO[redacted]ELIUS	CO[redacted]CH	1[redacted]1	31/1[redacted]2025	02[redacted]/2024	u[redacted]er.co	25[redacted]621	MO[redacted]N	AC[redacted]E
○	M[redacted]a	SA[redacted]A	2[redacted]2	31/1[redacted]2027	02[redacted]/2024	sa[redacted]m	11[redacted]	WE[redacted]	AC[redacted]E

Attention, fellows!
We are **R00TK1T**, have successfully penetrated the systems of the **global company Unilever** and now **hold the source code of your critical systems in our grasp.**
Your customer and supplier details are now under our control, and we are prepared to publish them on our private data channel.

Screenshot from R00TK1T's Telegram channel

In the R00TK1T's Telegram channel monitored by SOCRadar, the cyber attack announcement targeting Unilever shows severe risks to the multinational corporation and its ecosystem. The breach threatens to disrupt Unilever's operations and compromise sensitive data, impacting suppliers and customers. These kinds of attacks can lead to problems in other domains, such as legal and economic ones.

29 Mar
2024



March 29

JUST EVIL

Приятный доступ к базе сотрудников оборон сервиса Великобритании BAE Systems!

Продавать личные данные сотрудников (Полное досье: институты, сопроводительные письма, грамоты, сколько раз смотрел [redacted], должностные обязаности и тд.) не стал, а просто подарю их нашим заинтересованным в этих данных ведомствам.

Screenshot from Just Evil's Telegram channel

Just Evil, originating from the remains of the KillNet and led by its previous head, KillMilk, allegedly infiltrated the databases of BAE Systems, a significant entity within the aerospace and defense industries of the United Kingdom. This breach allegedly resulted in the acquisition of sensitive personal data of UK defense personnel, including detailed personal identifiers.

Given Just Evil's track record of cyber operations, targeting NATO countries during the Ukraine-Russia conflict under the banner of KillNet, the continued activities of this group present a persistent and concerning threat to Western states.

Ransomware Threats

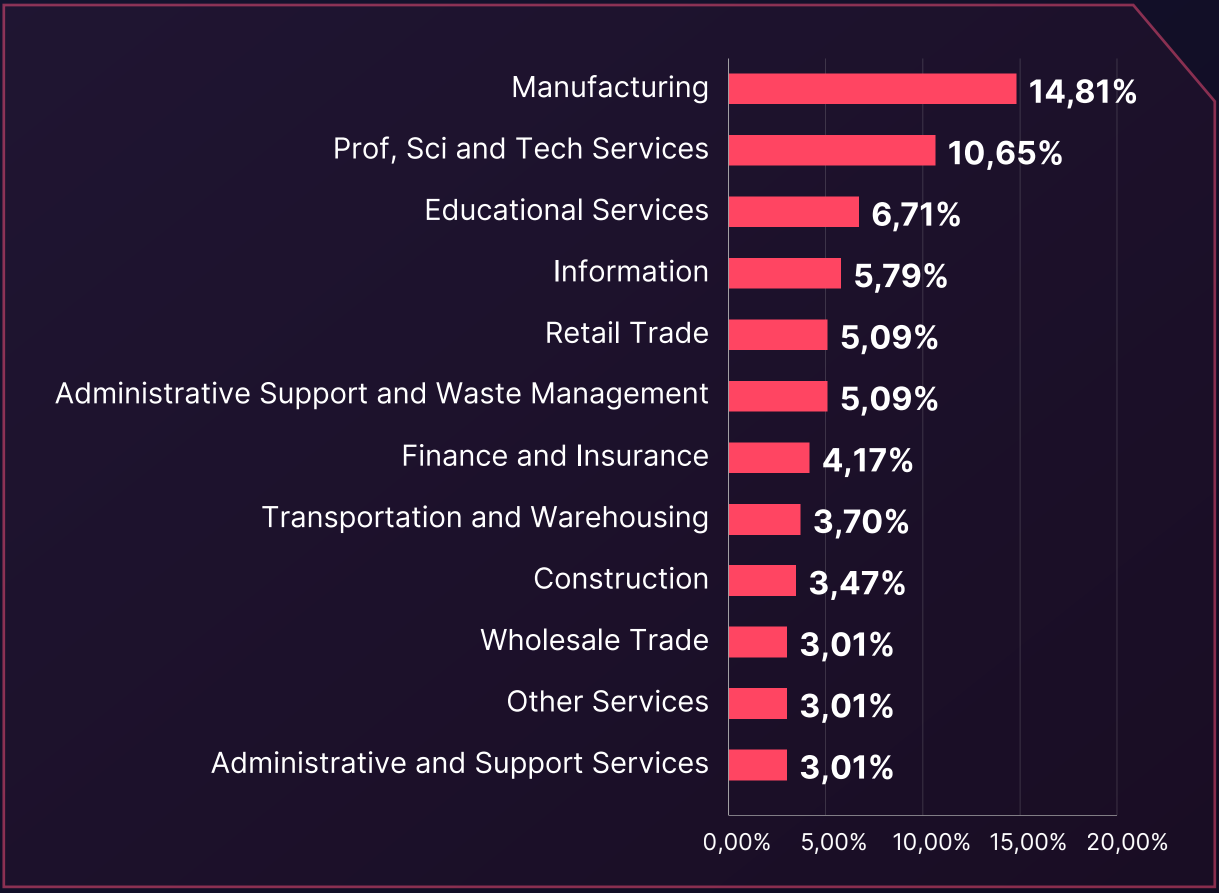
Ransomware attacks pose significant threats to organizations, frequently leading to critical consequences such as extensive data loss and the exposure of sensitive information.

There were 333 ransomware attacks where at least one entity from the United Kingdom was affected. It is equal to almost one ransomware attack a day throughout the year.

The manufacturing sector experienced the highest volume of ransomware attacks, constituting 14.81% of the total ransomware incidents encountered by British industries last year.

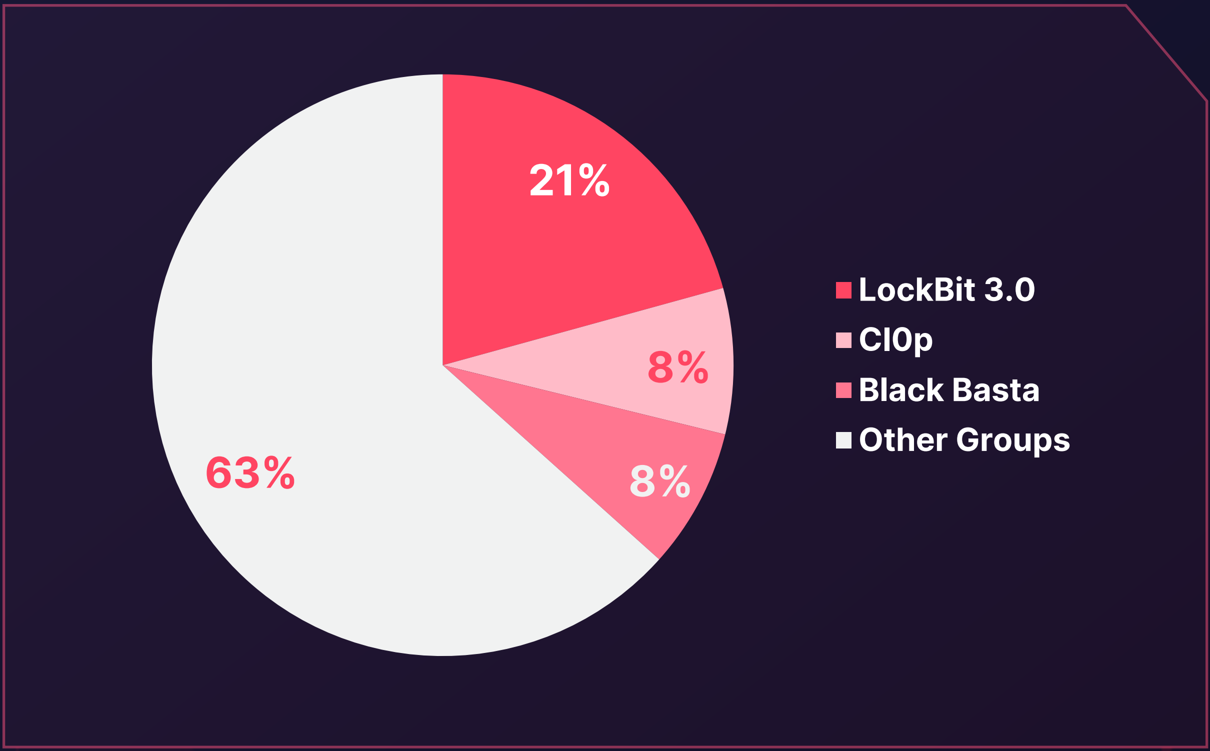
Closer Look into the Industries

Ransomware Attacks- Distribution by Targeted Industry



Top Ransomware Groups Targeting the United Kingdom

Top Ransomware Groups Targeting the United Kingdom



Lockbit 3.0 Ransomware Group

LockBit

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our blog post for more detailed information about the Lockbit 3.0 Ransomware Group.

Cl0p Ransomware Group

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Exploitation for Privilege Escalation:	T1068
Exfiltration Over C2 Channel:	T1041

Cl0p, a member of the well-known Cryptomix ransomware family, is a dangerous file-encrypting malware that intentionally exploits vulnerable systems and encrypts saved files with the ".Clop" extension. The name of the threat actor comes from the Russian word "klop," which means "bed bug," a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string "Don't Worry C|0P" found in the ransom notes.

On June 16, 2021, in a coordinated international effort involving law enforcement agencies from various countries, authorities arrested numerous individuals suspected of affiliation with the Cl0p ransomware gang. Despite this operation, the ransomware group grabbed attention a few days later by releasing data acquired from new victims.

You can visit our blog post For more detailed information about the Cl0p Ransomware Group.

Black Basta

Country of Origin: Russia

Black Basta is a ransomware group that has been active since April 2022 and they employ a double-extortion attack technique. The group was also observed to be linked to the FIN7(Carbanak).

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	North America and Europe
Target Sectors:	Manufacturing, Construction, Professional Services, Finance, Healthcare
Attack Type:	Valid Credentials, RaaS, Ransomware, Double-extortion

-TTPs-

Valid accounts:	T1078
Phishing: Spear-phishing attachment:	T1566.001
Exfiltration over C2 channel:	T1041

The Black Basta ransomware group emerged on the crime scene in April 2022 and swiftly cemented its position as a significant player in the cyber threat landscape.

The group sets itself apart through its rapid and decisive attack methodologies, focusing on various sectors, including manufacturing, financial services, and healthcare.

They are leveraging a Ransomware-as-a-Service (RaaS) framework. Black Basta employs double extortion methods, which is encrypting victims' data and threatening public release unless a ransom is met. Renowned for their effectiveness, the group swiftly executed several notable attacks following its establishment, exceeding 50 victims by the end of 2022. The ongoing activities of Black Basta show their capacity to inflict substantial disruptions on affected organizations.

You can visit our blog post for more detailed information about the Black Basta Ransomware Group.

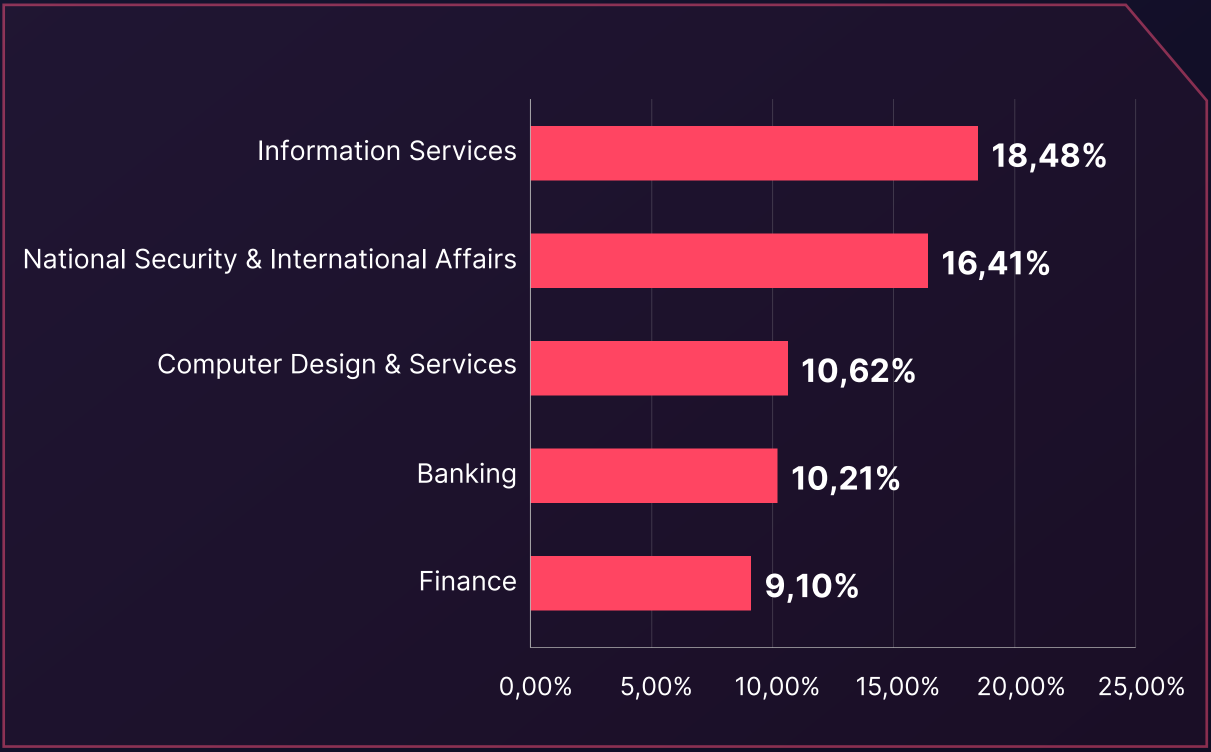
Phishing Threats

Phishing is one of the most effective methods to lure individuals into a dangerous spot. It allows threat actors to breach an organization without dealing with state-of-the-art security systems.

Over the past year, the United Kingdom has dealt with **16,610 phishing attacks**, primarily targeting the **Information Services** sector.

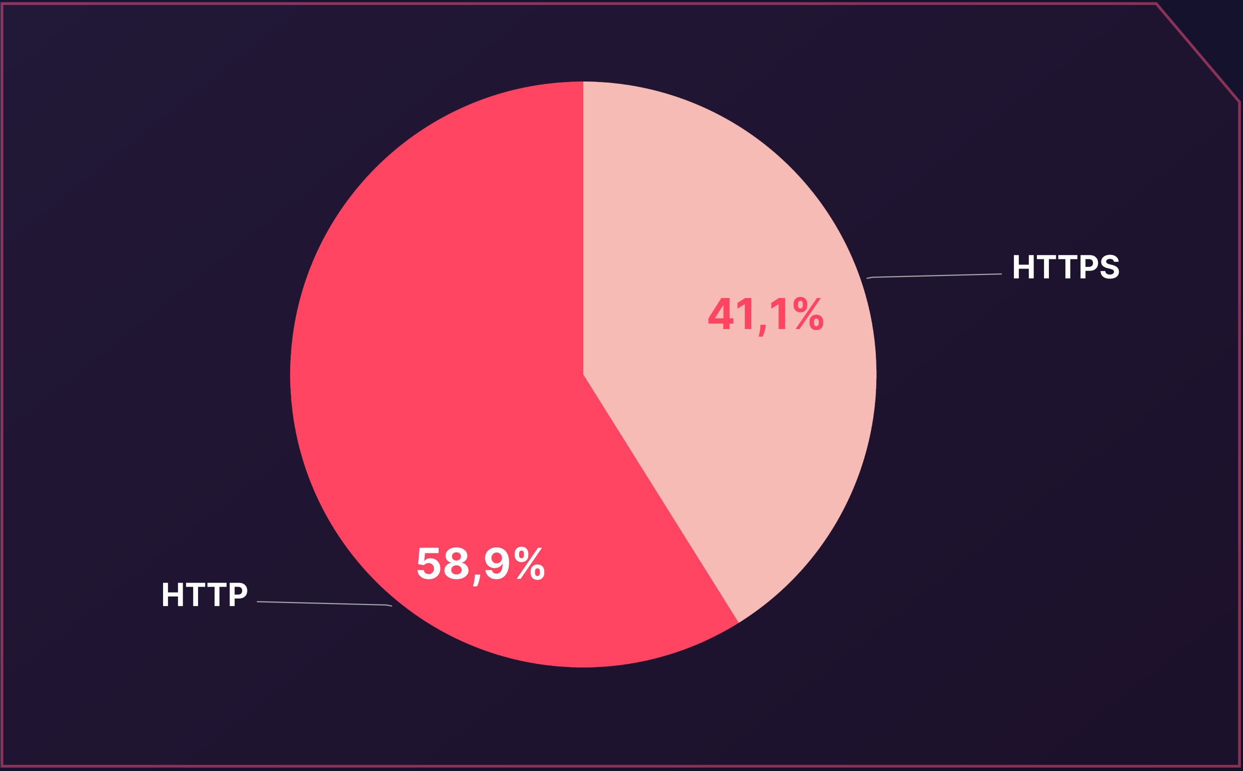
Deeper Look into the Industries

Phishing Attacks- Distrubution by Industry



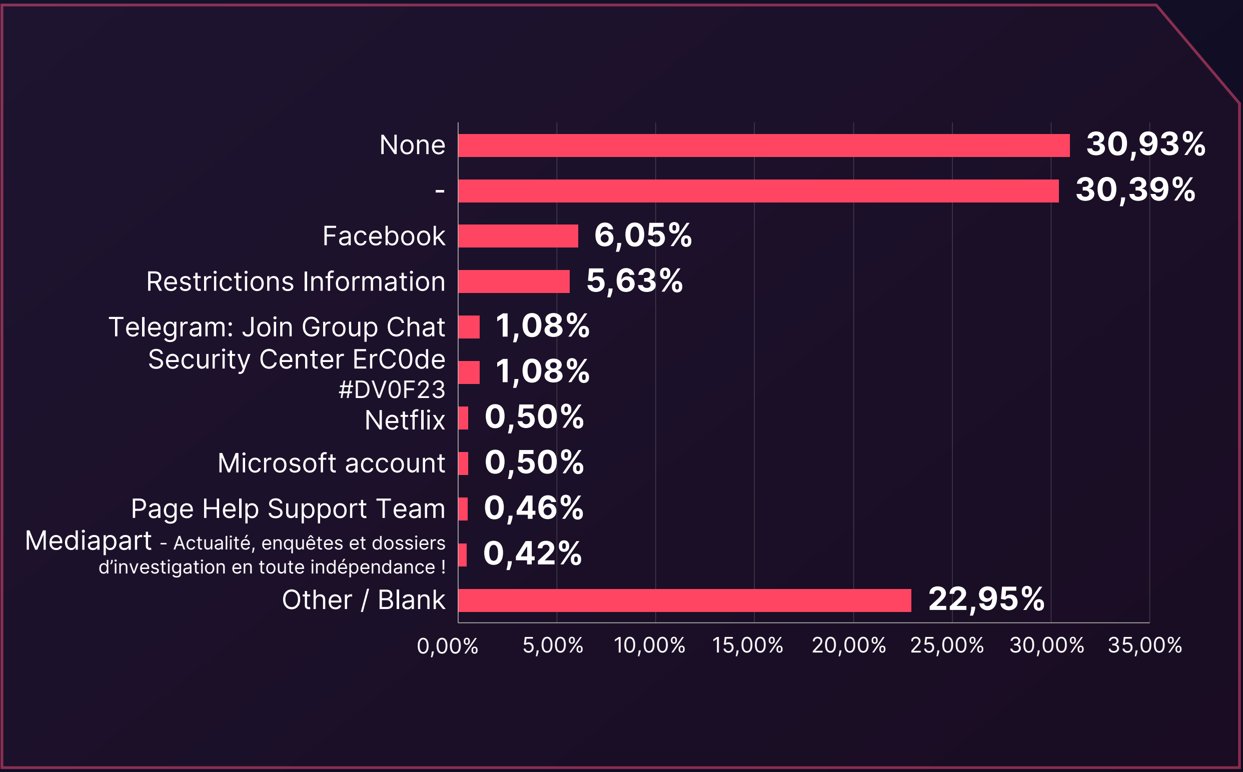
Distribution of Phishing Attacks Based on Security Protocols

Phishing Attacks - Distribution by SSL/TLS Protocol



Distribution of Phishing Attacks by Page Titles

Phishing Attacks - Distribution by Phishing Page Title



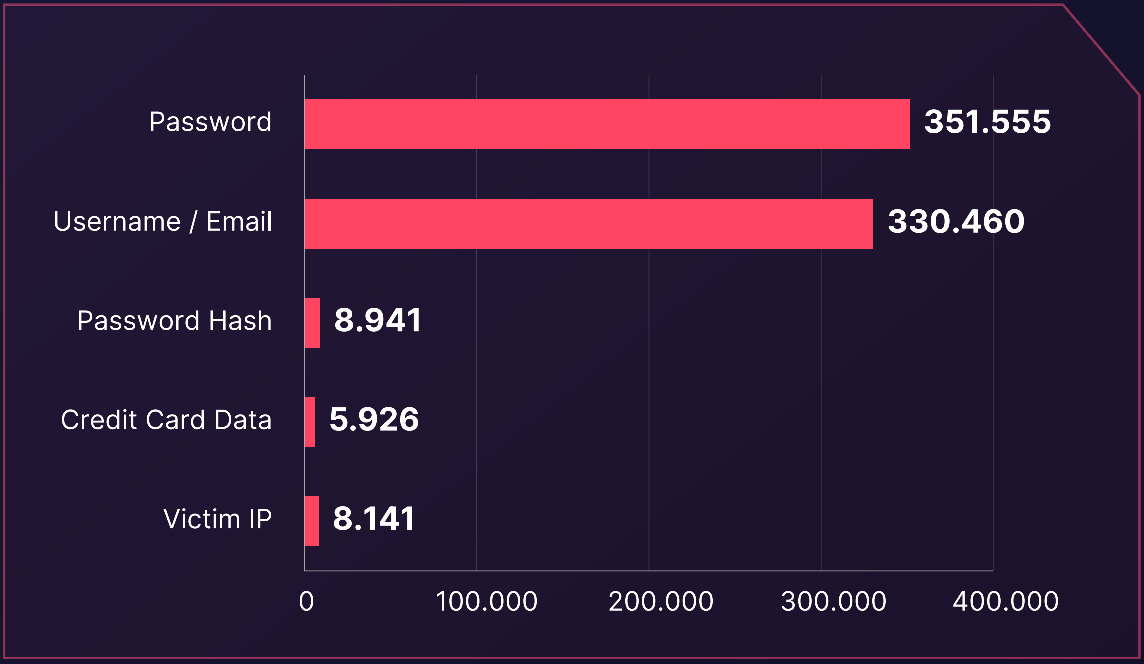
Stealer Log Statistics
Top Domains in the United Kingdom

Thousands of individuals' personal information, including passwords and credit card details, were compromised due to Stealer Logs. The following table presents the most frequently visited domains in the UK in 2023.

- amazon.co.uk
- bbc.co.uk
- dailymail.co.uk
- ebay.co.uk
- service.gov.uk
- www.gov.uk
- telegraph.co.uk
- rightmove.co.uk

The table below illustrates the distribution of compromised data retrieved from Stealer Logs across the most frequently visited domains in the United Kingdom.

Stealer Logs - Distribution of the Compromised Data



The data reveals a crucial reality about the compromised information. The many passwords and usernames that can be accessed show the significance of compromise throughout different domains.

These discoveries underscore the severity of data breaches, signaling organizations to bolster their security systems to safeguard personal information.

DDoS Attacks

DDoS Attack Statistics

The threat landscape back in 2023 was pretty active for the United Kingdom.

- The most expansive DDoS attack documented comprised **26 vectors**, featuring prominent techniques such as DNS Amp and TCP SYN attacks.
- The peak bandwidth witnessed during a DDoS attack reached **605.33 Gbps**, highlighting the significant capacity of these cyber threats.
- The highest recorded throughput during these incidents was **52.66 Mpps**, showing the rapid rate of data package transmission.
- DDoS attacks lasted for **32 minutes** on average, demonstrating the commitment behind the efforts to halt various services for half an hour, resulting in financial losses in some instances.
- **115,193 DDoS attacks** were recorded throughout the year, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for British targets.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks in 2023
DNS Amp	41,608
TCP SYN	19,914
TCK ACK	18,379
TCP RST	17,908
DNS	15,649

Top 10 Passwords

Using weak passwords equates to employing passwords already known by threat actors, thereby increasing vulnerability to unauthorized access and exploitation. These passwords, frequently sourced from easily accessible lists or swiftly cracked through brute force attacks, present minimal resistance to hackers.

Adopting strong passwords is imperative to ensure the security of both yourself and your organization. For this purpose, the Department for Science, Innovation, and Technology plans to ban tech with weak passwords.

Based on our research, the following table shows the most popular passwords in the UK by "hit count" showing how many times the following password has appeared.

Hit Count	Password
69,208	123456
56,413	password
31,578	liverpool
29,811	password1
26,968	123456789
22,221	qwerty
18,520	liverpool1
18,001	abc123
16,338	charlie
14,945	12345678

Recommendations

Strategic Recommendations

Enhanced Cybersecurity Measures: Organizations across all sectors, particularly retail and manufacturing, should prioritize the implementation of comprehensive cybersecurity measures, including regular vulnerability assessments and advanced threat detection capabilities.

Dark Web Monitoring: Establish proactive dark web monitoring capabilities to detect and mitigate potential data breaches, leaks, and illicit transactions involving sensitive information. Collaboration with threat intelligence providers can enhance visibility into dark web activities and enable timely threat response.

You can find out about the latest developments in the dark web with SOCRadar's Dark Web News module.

Ransomware Preparedness: Develop and regularly update ransomware response plans, including incident response protocols, data backup and recovery strategies, and communication procedures with stakeholders and law enforcement agencies. Conducting ransomware simulation exercises can help validate the efficacy of response plans.

Phishing Awareness Training: Implement comprehensive phishing awareness training programs for employees to recognize and report phishing attempts effectively. Simulated phishing exercises can assess employees' susceptibility to phishing attacks and reinforce security awareness across the organization.

Password Security Measures: Enforce strong password policies, including regular password rotation, complexity requirements, and the use of Multi-Factor Authentication (MFA) to mitigate the risk of credential theft and unauthorized access. Encourage the adoption of password management tools to securely store and manage credentials.

DDoS Mitigation Strategies: Deploy DDoS mitigation solutions and services to protect against volumetric, application-layer, and protocol-based DDoS attacks. Implement network traffic monitoring and anomaly detection mechanisms to detect and mitigate DDoS attacks in real time.

Enhance your DDoS defense with SOCRadar's DoS Resilience module.

Conclusion

Effective cybersecurity strategies require a keen understanding of the shifting tactics, techniques, and procedures (TTPs) employed by threat actors. UK organizations can utilize this report's findings to protect themselves from the top ransomware gangs.

Specific industries and their most significant threats are also covered in respective chapters. Phishing attacks pose a significant threat to Information Services, exploiting human vulnerabilities to gain unauthorized access. In the manufacturing sector, ransomware attacks loom large, disrupting operations and demanding hefty ransoms for data retrieval. For retail trade, on the other hand, finding sensitive information on the Dark Web is easy. Companies in those industries must act swiftly and take the necessary measures before their systems get compromised.

Early intelligence is paramount in this landscape where a new threat emerges constantly. Stealer Logs and Top Passwords are other problems organizations should address quickly since they are shared in plain text, waiting for attackers to just look at them. With the help of intelligence, companies can find out about their leaks and make the necessary changes. Proactively identifying potential threats allows organizations to implement essential safeguards before significant damage occurs.

Adopting a proactive, well-informed, and all-encompassing approach to cybersecurity is paramount. By partnering with advanced solutions like SOCRadar, organizations in the United Kingdom can enhance their defenses and navigate the ever-evolving cyber threat landscape more effectively.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies** in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

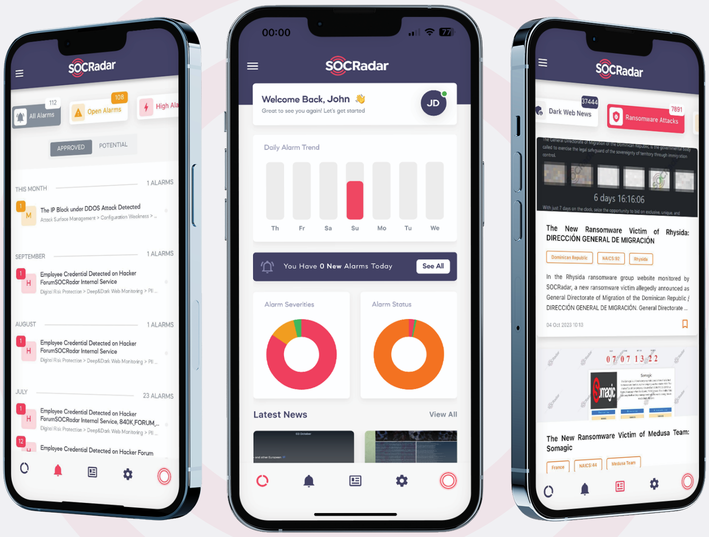
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



GET IT ON Google Play

Gartner Peer Insights™ Customer First

4.8/5 ★★★★★