



Cyber security in search

Analysis of Google search trends 2004 - 2019



redscan.com

Introduction

Google's annual 'Year in search' report offers fascinating insights into people's online search behaviour. At Redscan, we wanted to use Google's mass of search-related data to illustrate how the cyber security industry has changed over the last 15 years, including an examination of the people, events and trends that have shaped the industry.

Contents

1. The most searched in cyber security p.3

- 1.1 People
- 1.2 Companies, hacking groups and scams

2. Popular terminology p.5

- 2.1 The decline of network security
- 2.2 Cybersecurity or cyber security?

3. The biggest cyber security events of all time p.6

- 3.1 Data breaches
- 3.2 Most searched for data breaches by year
- 3.3 Threats and vulnerabilities
- 3.4 Biggest privacy stories

4. Technological changes p.10

- 4.1 The decline of traditional antivirus
- 4.2 The rise of endpoint and cloud security
- 4.3 The popularity of SIEM
- 4.4 Passwords and authentication

5. The threat landscape p.13

- 5.1 Threat types
- 5.2 Cryptojacking

6. Compliance p.14

7. Future trends p.15

- 7.1 On the rise
- 7.2 The future of the cyber security profession

1. The most searched in cyber security

1.1 People

Every year, Google reveals the most searched for music artists, athletes and actors, but we were interested to identify the most popular personalities in cyber security and how their popularity compares to other celebrities.























What we say

“Cyber security professionals may not be as glamorous as rock stars or A-list actors, but it’s clear that well-known faces within the industry are becoming more mainstream. Robert Herjavec and John McAfee comfortably take the two top spots in our list, but Troy Hunt’s popularity as a security researcher, blogger and founder of Have I Been Pwned means that he is increasingly searched for online.

“Of the most searched for cyber security experts on the planet, it’s a sad truth that the top five is exclusively white and male. The industry is in desperate need of more female figureheads and individuals from a broader range of backgrounds. Jane Frankland and Poppy Gustafsson are examples of excellent female role models within the industry, but more needs to be done to address the gender imbalance.”

1.2 Companies, hacking groups and scams

We’ve also analysed and compiled a list of the most searched for cyber security technology companies, hacking groups and phishing scams (2014-2019).

Top five	Pure play cyber security companies	Pure play cyber security companies (enterprise)*	Hacking groups	Phishing scams^
1.	 Norton	 Symantec	 Anonymous	 Apple
2.	 Avast	 Fortinet	 Lizard Squad	 PayPal
3.	 AVG	 Akamai	 LulzSec	 HMRC
4.	 Kaspersky	 Mimecast	 Chaos Computer Club	 Amazon
5.	 Eset	 FireEye	 Syrian Electronic Army	 NatWest

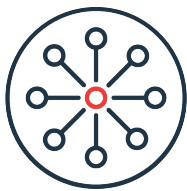
*Only includes companies without a consumer offering

^Based on UK search data only

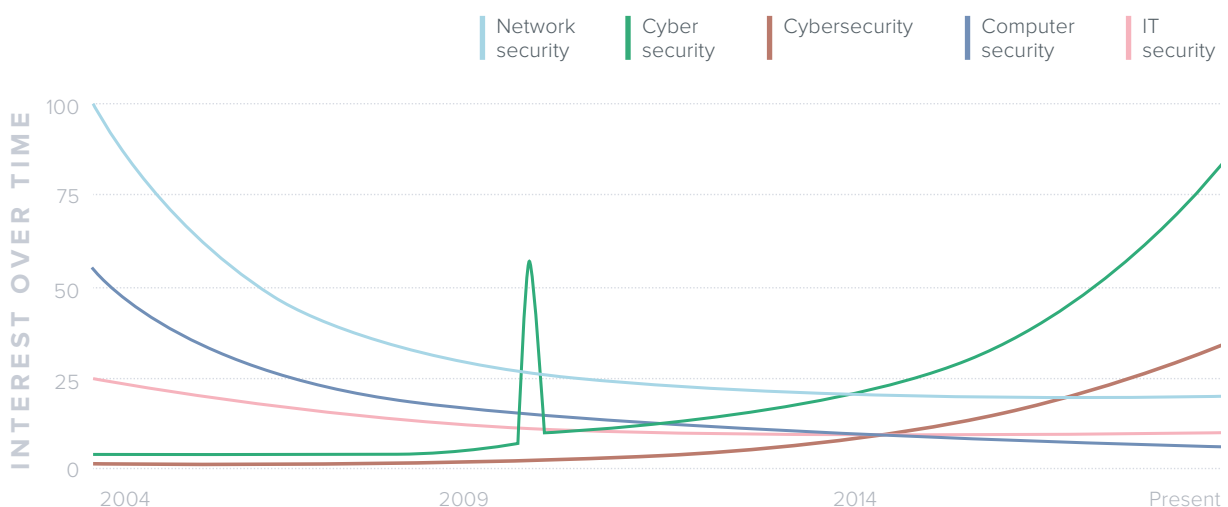
2. Popular terminology

Few people would dispute the extent to which cyber security has changed over the last decade. What can search behaviour tell us about how technologies, trends and even the language of cyber security have evolved?

2.1 The decline of network security



Understanding how people talk about security can be highly revealing. In 2004, 'network security' was a common search term but its use has gradually decreased in favour of 'cybersecurity' and 'cyber security'. 'IT security' is more widely searched for in Germany and Austria but its use elsewhere is limited. We're not completely sure why there's a sudden spike in searches for 'cyber security' in October 2009. One possible explanation is then US president, Barack Obama, proclaiming National Cyber Awareness Month.



2.2 Cybersecurity or cyber security?

Whether cyber security should be one word or two has long been a bone of contention, but maybe search data can settle this matter once and for all. We discovered that in most parts of the world, cyber security is most commonly spelled using two words. 'Cybersecurity' is searched less often, but slightly more frequently in the US than the UK. Searches for 'cyber-security' are virtually non-existent.

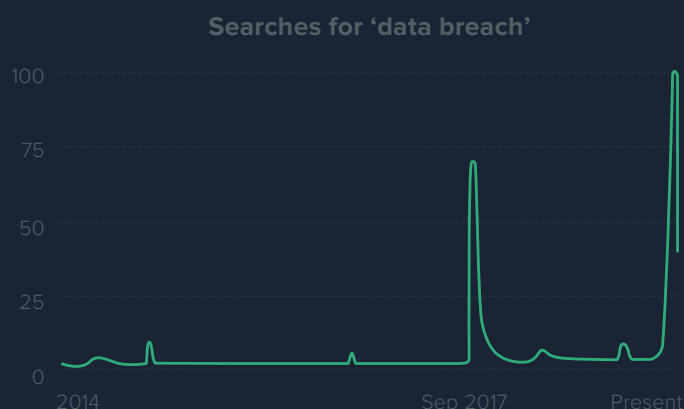
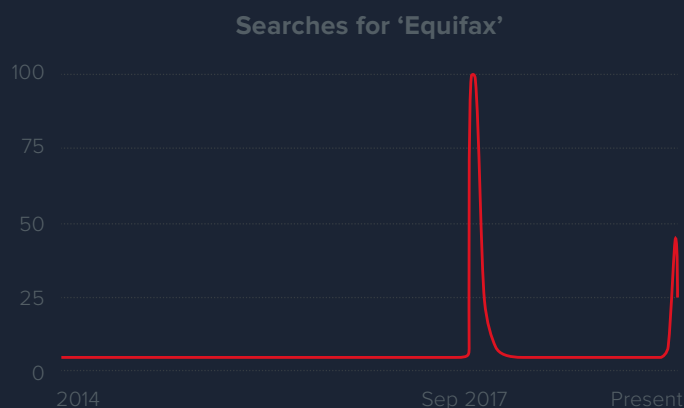
3. The biggest cyber security events of all time

With so many massive cyber security stories in the news over the last 15 years, we were interested to see which data breaches, vulnerabilities and privacy violations have received the most online searches.

3.1 Data breaches



The most searched for data breach in the last decade is the 2017 Equifax breach, likely testament to the number of people affected and the value of the data compromised. The fact that Equifax disclosed the breach late and communicated details poorly may also have had an impact on search behaviour, driving people to find out whether their details had been stolen. Indeed, interest in the Equifax data breach is so high that it skews all historical searches for the term 'data breach'.



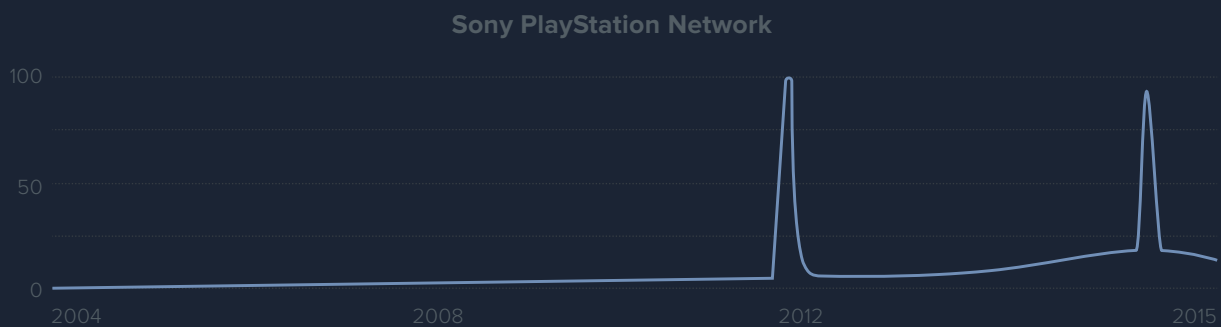
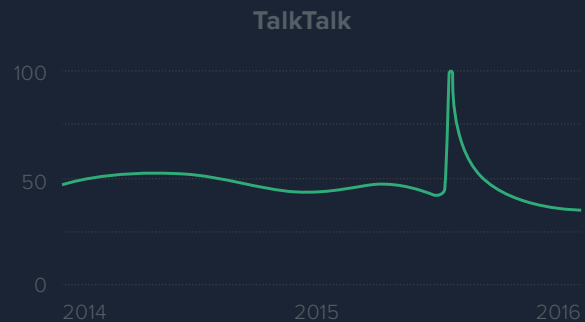
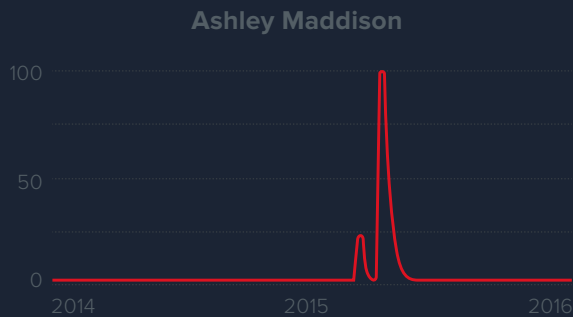
Equifax breach stats

- 148 million people affected, including 693,665 UK citizens
- Personal data stolen included names, addresses, driving license and social security numbers
- Three senior Equifax executives sold stock worth almost \$1.8 million in August 2017 before the breach was made public on Twitter in September 2017



- Richard Smith stepped down as CEO in September 2017

Other highly searched data breaches are:



3.2 Most searched for data breaches by year

2019



Collection #1
January

2018



Marriott
November

2017



Equifax
September

2016



Yahoo
September

2015



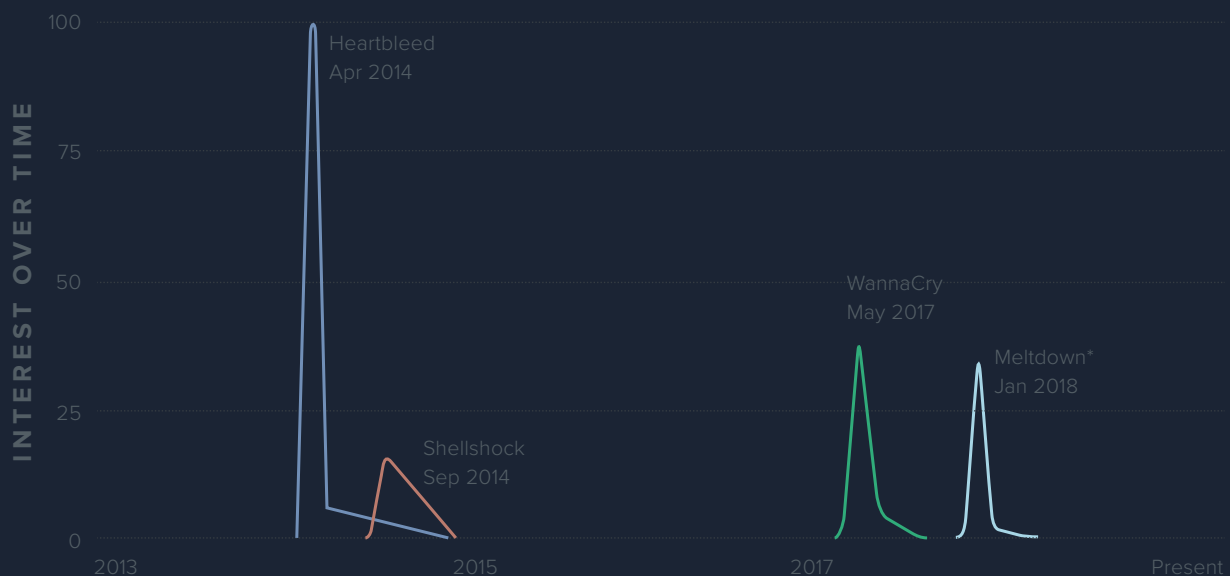
Anthem
February

To understand the most searched for data breaches by year, we looked for the biggest spikes for 'data breach' in each calendar year and cross referenced these spikes with data breach reports.

3.3 Threats and vulnerabilities



Numerous cyber security threats and vulnerabilities have made the news in recent years. Our search analysis over the last decade reveals that Heartbleed, a security bug affecting approximately 500,000 web servers, generated the biggest spike in search interest. WannaCry, which in 2017 caused massive disruption to the NHS, and Meltdown, a hardware vulnerability affecting microprocessors, are second and third on our list.



*Searches for the Spectre vulnerability (associated with Meltdown) cannot be visualised with Google Trends data due to the popularity of the 2015 James Bond film 'Spectre'

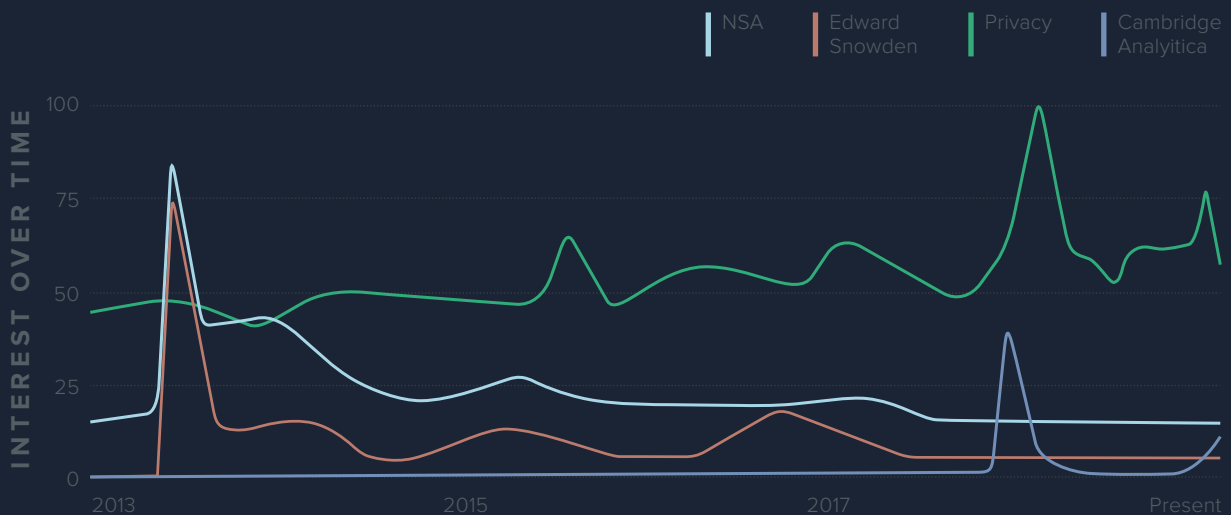
What we say

"The disruption and damage breaches can cause means that swiftly detecting and responding to them has never been so important. Businesses need to learn from the mistakes of organisations such as Equifax and ensure that if they suffer a breach, they have appropriate procedures in place to report it to regulators as well as communicate the risks to all individuals affected."

3.4 Biggest privacy stories



In recent years, internet privacy has come under the spotlight. The NSA Snowden revelations in 2013 were a watershed moment, resulting in massive search volumes for 'Edward Snowden' and 'NSA'. Searches relating to the 2018 Cambridge Analytica scandal appear lower in volume, but this is likely clouded by Facebook's involvement in the incident. Searches for 'privacy' peaked soon after the Cambridge Analytica story broke.



What we say

"The Cambridge Analytica scandal is just one in a long line of high-profile stories that highlight the importance of internet privacy. In the aftermath, millions of people deleted their Facebook account. But Facebook isn't the only company accused of collecting and misusing data and people must ensure that they continue to be mindful of the information they share and regularly review their privacy settings."

"Since the GDPR, organisations now have a greater responsibility to ensure that they have a lawful basis for processing data and make it clearer to individuals about how their data will be used and why. The GDPR is helping to redress the digital imbalance between companies and individuals but we need governments and regulators to do more to ensure online privacy is protected. We've seen the consequences when we allow tech giants to regulate themselves."

4. Technological changes

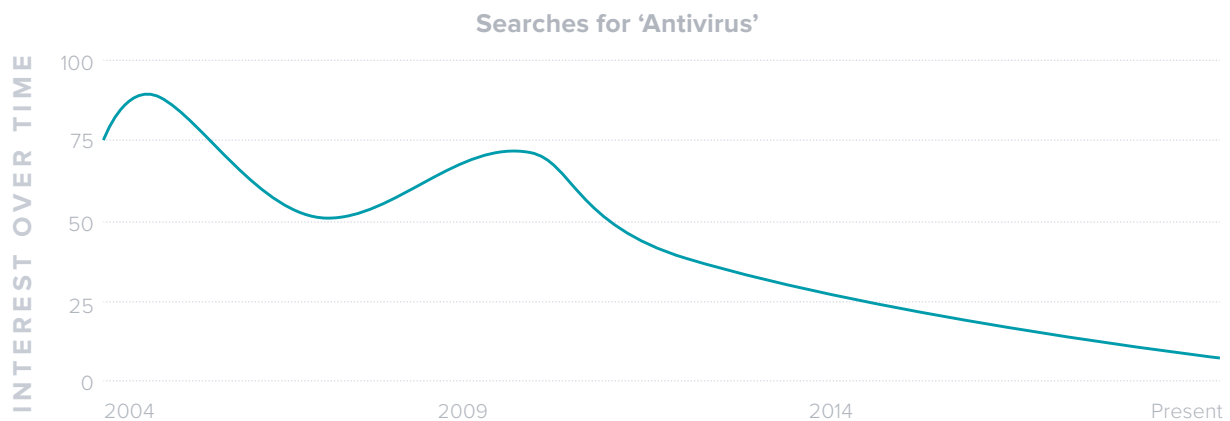
Technological evolution impacts cyber security in a fundamental way. Businesses embracing the Cloud, Internet of Things (IoT) and Bring Your Own Device (BYOD) need to ensure that they have appropriate controls in place to defend their infrastructure, systems and data against the latest threats.

4.1 The decline of traditional antivirus

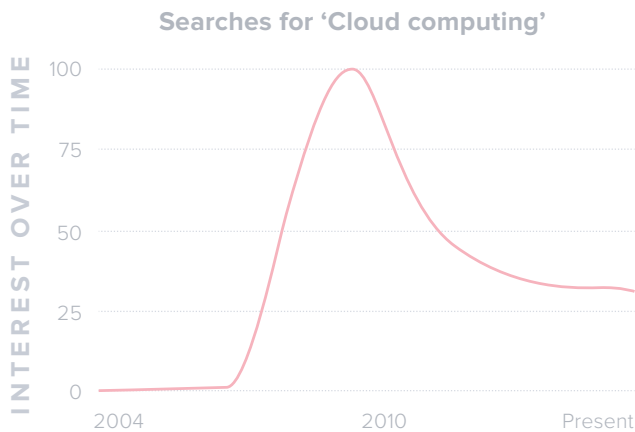


15 years ago, antivirus (AV) software was a key solution businesses relied upon to prevent threats; brands like McAfee, Kaspersky, Norton, Avast and AVG were household names. Today, there are many more vendors and a growing acceptance that traditional AV solutions are no longer enough – organisations need a range of security technologies.

Google's data shows that interest in all the main AV brands has faded over time. Even the erratic behaviour of its founder has done little to keep McAfee in the news, despite its claims to be the world's largest dedicated security technology company.



4.2 The rise of endpoint and cloud security

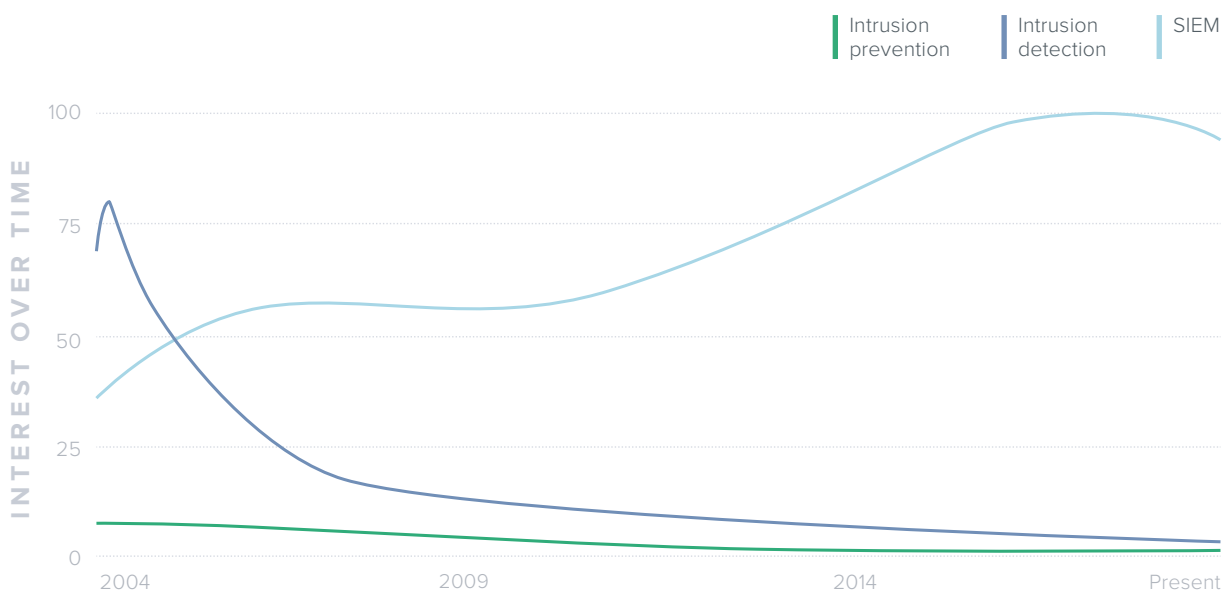


A decline in searches related to traditional AV tracks with the decrease of 'network security' (see section 2.1) and rise of next-generation security and behavioural monitoring solutions.

Key search terms gaining in prominence over the last decade are 'Cloud Computing', 'Mobile Device Management' (MDM) and 'BYOD'. In particular, the search volume for BYOD has grown significantly over the last few years.

4.3 The popularity of SIEM

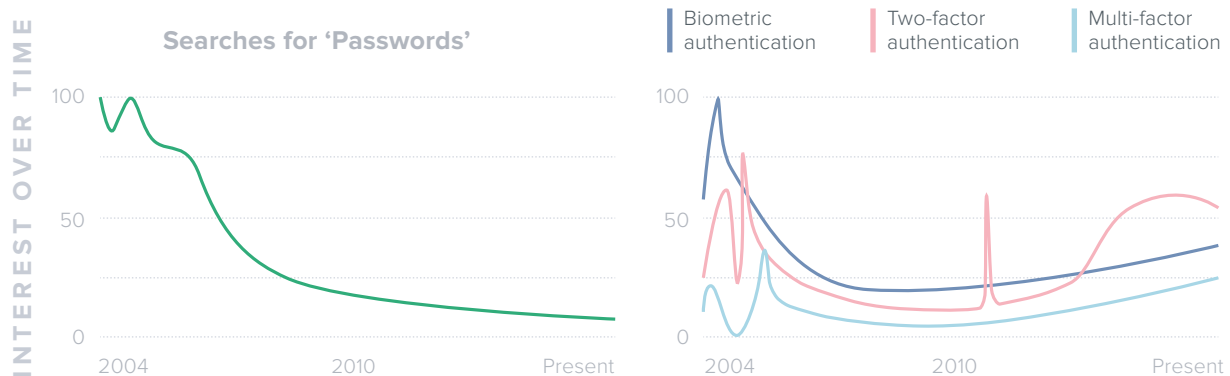
Analysis also reveals that searches for traditional perimeter security technologies such as firewalls and intrusion detection systems began to decline in the late noughties. Interestingly, searches for 'SIEM' (Security Information and Event Management) have doubled since 2004, despite some commentators questioning the future of the technology.



4.4 Passwords and authentication



The need for individuals to set strong account passwords remains fundamental to cyber security yet our analysis reveals that searches for 'passwords' is on a sharp decline.



What we say

"As businesses embrace the cloud and use more endpoint and IoT devices, traditional security solutions are no longer sufficient. Organisations now need a range of technologies to protect the network against advanced threats, as well as swiftly detect and respond to threats able to breach it. Despite many commentators questioning its future, SIEM continues to be important for this reason."

"It's a bit concerning that searches for passwords are in such a steep decline. Good password hygiene is essential, and people are often really bad at setting unique passwords."

"Other authentication trends are slightly easier to explain. We see the most interest in biometrics and multi-factor authentication in the early 2000s when these technologies first emerged. A rise in the last five years is likely explained by more online services now relying on these solutions to provide an extra layer of security. We believe that the search spike for 2FA in August 2012 corresponds with Dropbox implementing this authentication method for the first time."

5. The threat landscape

As the technology landscape changes, cybercriminals are quick to take advantage by exploiting new vulnerabilities and developing more sophisticated attack techniques. We see this clearly when examining search interest around traditional and modern attack vectors.

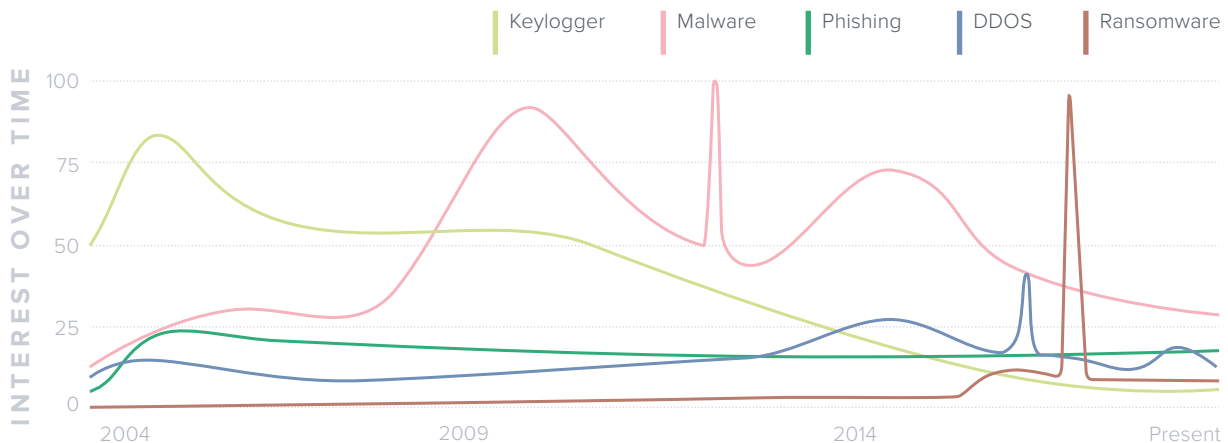
5.1 Threat types



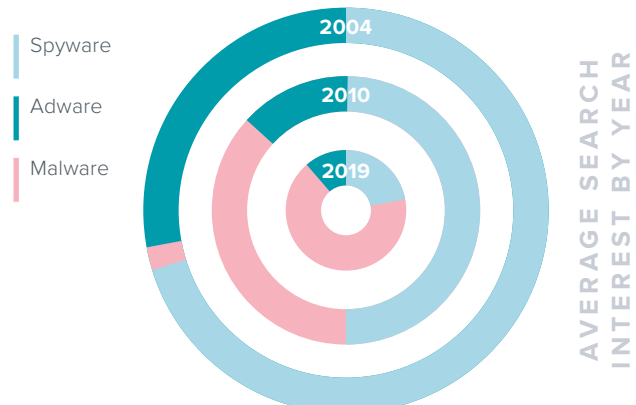
Interest in keylogging programs, software designed to record user keystrokes, peaked in 2005 and has been in decline since. This is likely due to cybercriminals having now devised ways to intercept data en masse.

Interest in Distributed Denial of Service (DDOS) attacks has remained remarkably consistent over the last 15 years, peaking around major attacks such as those targeting Xbox Live in December 2014 and Dyn in October 2016.

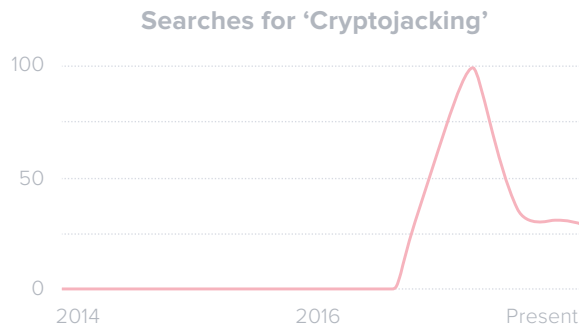
No spike in search data, however, is as large as the one for 'ransomware' at the point of the WannaCry outbreak.



We were surprised to see the extent to which 'spyware' and 'adware' once dominated searches compared to 'malware' - with scores of 76/100, 31/100 and 2/100 respectively in 2004. Fast forward to 2010 and the searches for spyware and adware decrease to 11/100 and 3/100, while malware is up to 8/100. Today, the scores are even lower, but malware has a higher percentage of searches among the four terms - 1/100, <1/100 and 3/100.



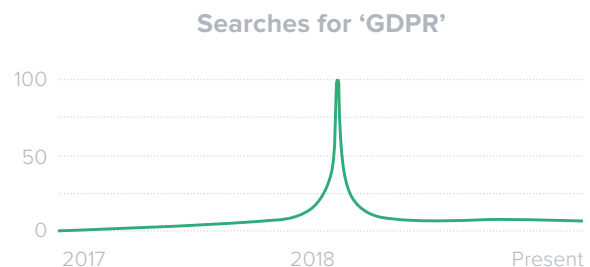
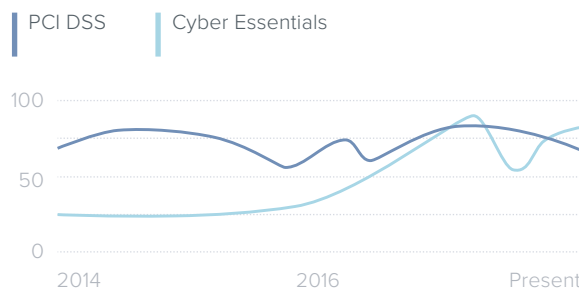
5.2 Cryptojacking



Cryptojacking involves cybercriminals compromising computing resources in order to mine cryptocurrency. Given that cryptojacking can be difficult to detect, it is now a popular alternative to ransomware. While the volume of cryptojacking searches does not compare to more widely known threat types (such as those identified in 5.1), we thought use of the term warranted analysis.

6. Compliance

Examining UK searches relating to data and information security regulations and standards tells an interesting story. Search data reveals that interest in the PCI DSS and Cyber Essentials has remained steady over the last five years. In contrast, interest in the GDPR rose incredibly sharply in the months prior to its enactment in May 2018 and has quickly declined since.



What we say

“A huge spike in searches for the GDPR in the weeks prior to its enactment reveals a lot about the widespread panic that the regulation created. Now that the deadline has passed, many businesses believe that the hard work has been done. In reality, compliance is an on-going effort that requires constant reassessment. Just because an organisation satisfied requirements a year ago, doesn’t mean it’s still compliant one year on.”

“A lot of the challenges that existed prior to the GDPR’s implementation still exist today. In fact, due the evolving security landscape, these challenges are now greater than ever. Large scale breaches persist because organisations still don’t take appropriate measures to prevent, detect and respond to them.”

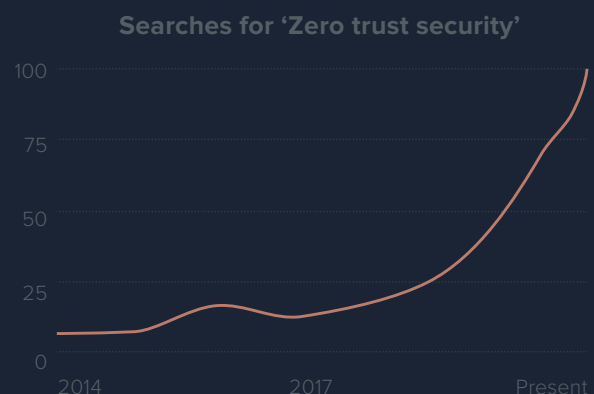
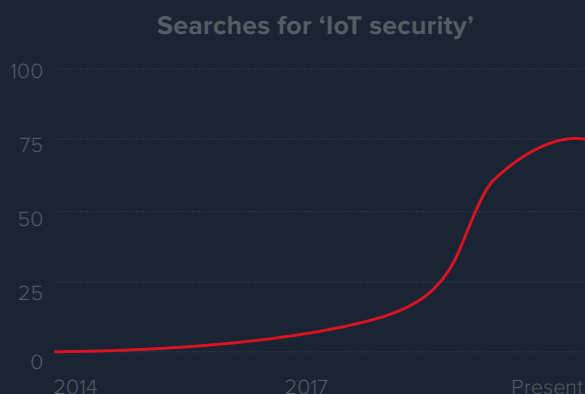
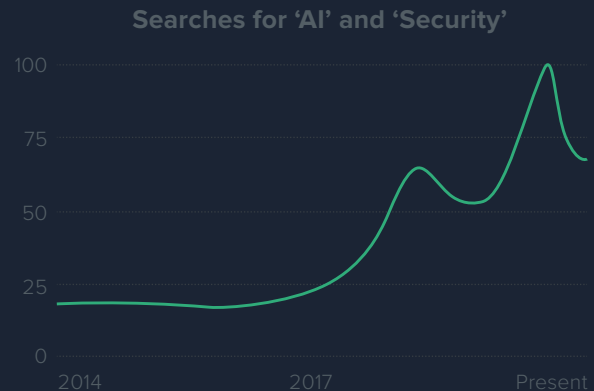
7. Future trends

To keep pace with cyber threats, it's important that the security industry continues to embrace new technologies and strategies. We used Google's data to identify the trends that are driving organisations within the sector and examine whether attempts to address the current skills crisis by recruiting more people into the industry are having an impact on search behaviour.

7.1 On the rise

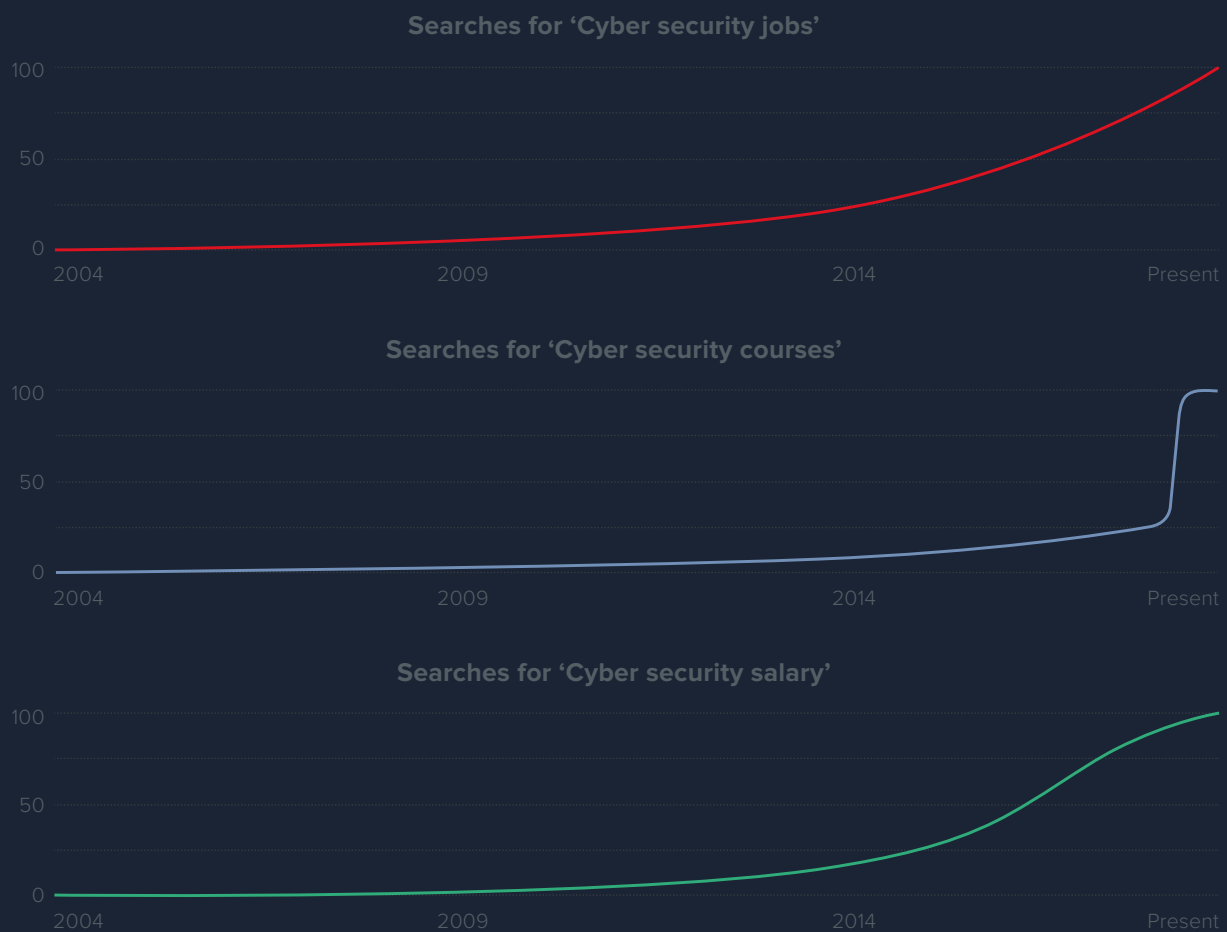


Our analysis reveals that searches relating to cyber security industry trends such as 'Threat hunting', 'AI Security' and 'Zero Trust Security' have grown considerably in the last five years. Unlike searches relating to specific cyber threats, which tend to demonstrate huge spikes in interest (see section 5), interest in these trends is growing steadily and, we believe, will continue to do so.



7.2 The future of the cyber security profession

Given the current cyber security skills crisis, it's interesting to see a significant increase in searches for 'cyber security jobs' and 'cyber security courses' over the last three years. Searches for 'cyber security salary' have also grown steadily.



What we say

"The massive shortage of cyber security professionals is undoubtedly creating many challenges for businesses – there just aren't enough qualified experts around to support the rising global demand. While it's pleasing to see that interest in cyber security jobs and education is increasing, more needs to be done still to attract and train new talent."

Conclusion

As our Google trends research shows, interest in cyber security-related events, issues and solutions has never been greater.

The rising number and increasing sophistication of cybercriminals and nation-state hackers continues to present enormous challenges for businesses, with often catastrophic results. Equifax is now synonymous with its 2016 data breach and a case in point for the need to ensure that appropriate resources are in place to prevent breaches and the financial and reputational damage associated with them.

Despite all the technological change that has taken place in the industry during the last 15 years, there is still no silver bullet for security. Traditional solutions that business have relied upon for years are declining in popularity, in favour of next generation tools that incorporate advanced behavioural monitoring, AI, automation, and response.

Technology is only one part of the solution to protect businesses, however. To tackle the latest threats, people remain as important as ever. Employees need to be educated about cyber security best practice, such as setting strong passwords, and trained to spot the tell-tale signs of attacks.

It is encouraging that interest in the cyber security industry as a career option appears to be growing. The global skills crisis is one of, if not the single biggest challenge the industry faces, as well as perhaps the hardest to solve in the short term. The more training and resources available to encourage people to enter the profession, the better businesses will be able to safeguard against threats for the next 15 years and beyond.

Disclaimer

The purpose of this report is to provide an overview of cyber security online search trends. Due to the difficulty of analysing searches based on keywords alone, owing to spelling differences and word ambiguities, it is not always possible to draw concrete conclusions from the data. If you believe any aspect of the report is inaccurate, please get in touch and let us know. Search data correct as of 16th August 2019.



About Redscan

As a provider of managed security services, Redscan delivers the capabilities organisations need to protect their assets from advanced cyber-threats, 24x7. By thinking like the adversary, leveraging the latest detection technologies and intelligence, and offering clear advice, our cyber security experts help organisations of all sizes to expose and address vulnerabilities plus swiftly identify and shut down attacks. Services offered include Managed Detection and Response, CREST-accredited Penetration Testing and Red Team Operations.



Call us

0800 107 6098



Email us

info@redscan.com



Twitter

[@redscan](https://twitter.com/redscan)



LinkedIn

[/redscan](https://www.linkedin.com/company/redscan)

Redscan is a trading name of Redscan Cyber Security Limited. All rights reserved 2019. Company number 09786838. Google and the Google logo are registered trademarks of Google LLC. All other product names, trademarks and registered trademarks are property of their respective owners.

Front page images licensed under CC BY 2.0: Edward Snowden credit Laura Poitras / Praxis Films | Mark Zuckerberg credit A1Cafe | John McAfee credit Gage Skidmore