What is OSINT?

OSINT is intelligence “drawn from publicly available material”(CIA).

OSINT, short for Open-Source Intelligence, is **data that has been obtained from publicly available sources**, that are accessible without payment. OSINT is widely used within law enforcement work, cybercrime activities such as planning an attack, or for business operation purposes, such as checking out the competition. Let’s explore some examples of OSINT data:

- **A company that has a public web page that introduces some/all of their employees** (think a “meet the team!” page). An attacker could use this to very easily gather a list of targets for social engineering attacks. Some sites may even include contact email addresses or phone numbers, which can aid the social engineering process dramatically.
- **Job Descriptions that leak information about a company’s internal systems** (example: a system administrator role requiring experience with Windows Server 2016 and Solaris). An attacker can use this to plan internal attacks, lateral movement, and privilege escalation once they have gained a foothold in the network.
- **Photos on social media that are geotagged and contain device information in the metadata** (example: that nice photo you shared on holiday? we can find where that is, usually in a matter of seconds – and the device you took it on).
- **Reading a user’s social media profile to build up a profile of them** (information such as date of birth, locations, friends, interests, family). This can be used to learn more about an individual, which is commonly done pre-interview so that employees can get a sense of how the person will act in the workplace.
- **Exposing Cyber Criminals.** Whilst this begins to move into the Threat Intelligence domain, it is possible to use OSINT sources and social-engineering skills to identify the true identity of cybercriminals and pass the details to law enforcement.

As you can see, the above can be useful to both attackers and defenders. Attackers can build up a good picture of their target without directly interacting with their systems, whilst defenders can get a sense of the publicly available information that is present on the internet, and work to reduce this or mitigate it using security controls such as user awareness training and social-media policies.

Why is it Useful?

Lots of people can benefit from utilizing OSINT. Below, we’re going to explore some different groups and how they could use publicly available information to their advantage.

For Defenders:

By looking at the information that is available on the internet, defenders can take steps to reduce this or implement other controls that will mitigate attacks or reduce their effectiveness. If an attacker was able to build a detailed profile on an employee, this could be very dangerous. However, if that employee has had security training, then they will potentially be better at spotting malicious emails and social engineering attacks. By removing information online that may aid an attacker, the defenders are reducing the attack surface, which is the total area that an attacker could exploit to gain access to internal systems. This activity is often referred to as conducting public exposure assessments. Examples include gathering information employees put on social media, identifying internet-facing assets, DNS checks, finding old login portals or websites, and much more.

For Attackers:

As we previously mentioned in the last lesson, OSINT sources can be a great way to discover information about a target company or individual. By working out what systems a company uses, the right exploits and attack methods can be planned out in advance. Employee information can be harvested, allowing potentially effective social-engineering attacks, and spear-phishing email campaigns to be conducted, tailored to their intended targets to make them more believable. An Organization should be careful about what information their systems and employees are sharing online. The process of collecting this information for malicious purposes is commonly referred to as target information gathering, or passive information gathering (because the attacker is not directly engaging with the target's systems, such as port or vulnerability scanning).

For Law Enforcement:

Government and Police organizations will utilize OSINT to track persons of interest, such as criminals, suspects, and terrorists. Profiling is the activity of collecting information on an individual to build up a picture of their personality and behavior. This can be used to predict where they will be at certain times, based on interests and previous locations. OSINT can be used to uncover the identities of cybercriminals that have poor OPSEC (operational security – the practice of hiding yourself online by disassociating your online persona with your real self). It can also be used to help find missing persons (a great example of this is Trace Labs, a non-profit organization that hosts online OSINT CTFs, which work to track missing people and assist law enforcement).

For Businesses:

Businesses can utilize OSINT to keep an eye on the competition, watch for market activity, learn more about their customer and how to best engage with them, improve business operations via data enrichment, and also monitor for security risks such as leaked credentials, employees sharing confidential information, or hackers planning attacks.

Intelligence:

Getting data through the web is not enough, you also must be able to identify what you got, process all that data, and determine which data is useful or not. That will help you to generate knowledge and, above all, you will achieve the main goal of any intelligence operation… Obtain relevant resources that can help you in your decision-making process.

In this section, you will learn about the most crucial and fundamental element of the Intelligence process, a methodology called *The Intelligence Cycle*. This will help you to improve your investigative skills and will raise all your intelligence operations to the next level!

The Intelligence Cycle:

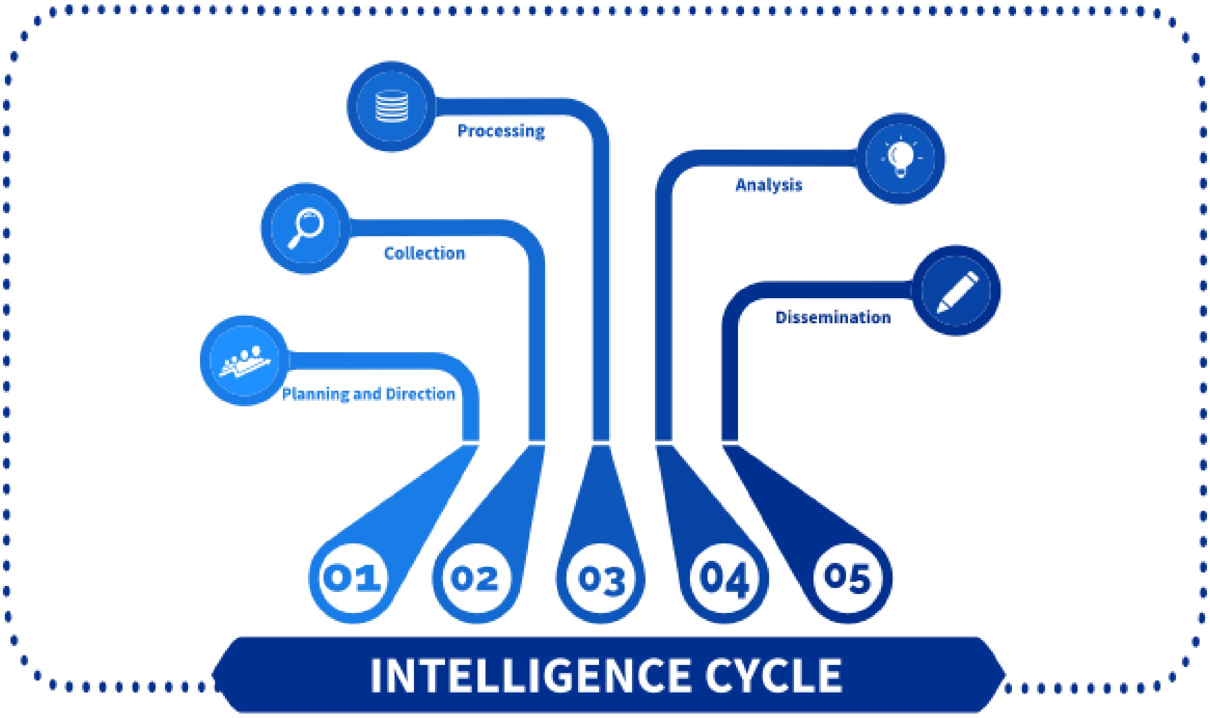
It doesn't matter if you are a member of a law enforcement agency or a security analyst for a company, either way, when you are in an intelligence scenario you will likely be facing the same landscape. On one hand, you will have a huge amount of data that must be analyzed, and on the other, you will have a problem that must be solved.

When dealing with this scenario you need to take advantage of the massive amount of data at your disposal and use it to create an intelligence report that provides a clear explanation of the solutions you are looking for.

The only issue here is that intelligence reports do not grow on trees. So, you must not only identify all this data but also classify and organize it in such a way that all this data can be converted into information.

For these situations, there has always been a process of knowledge creation called *The Intelligence Cycle.* This iterative model describes a series of stages and procedures that a researcher has to perform to convert the collected data and information into intelligence products capable of bringing solutions to the organization.

This process is carried out in 5 fundamental steps, which are shown in the below image:



PHASES:

1) Planning and Direction.

This first stage is the crucial element of the research process, it is the moment when you define which horizon will your investigation take.

This is where you determine the purpose of your research and what kind of information you are looking for.

2) Collection (gathering of data and information).

In this second phase your objective will be the identification of which kind of processes you will use to carry out the collection of such information, and then, using all the techniques you know, obtain the data that will help you carry out your intelligence operation.

3) Processing of data and information.

In this phase, you will take care of all that was obtained in the previous process.

Here your objective is not only the visualization of the information but also the application of decoding, decryption, validation, and evaluation techniques that will allow you to filter the huge amount of information you obtained, to identify useful data for your research.

4) Analysis to produce meaningful intelligence.

This is where analysts can show what they really are.

Here you must compile all the information you filtered in the previous step to obtain the solutions to your initial problem, as well as the creation of a coherent intelligence product (report, conference, etc.) that allows you to clearly explain the process you recently carried out

5) Dissemination of intelligence to the clients.

And finally, we have the final step. Here you must deliver the product you developed throughout the process to the stakeholders (individuals or groups) that requested it. This will help these people make informed and appropriate decisions when tackling the original problem.

That is all about the intelligence cycle, now you know everything you have to know to carry out an intelligence process and succeed in the process.

If you want to know more about this topic you should check the following links:

- https://www.intelligencecareers.gov/icintelligence.html
- https://www.sciencedirect.com/topics/computer-science/intelligence-cycle
- https://www.e-education.psu.edu/sgam/node/15
- https://www.groupsense.io/resources/how-to-use-the-intelligence-cycle-to-secure-your-brand

Tools and Services

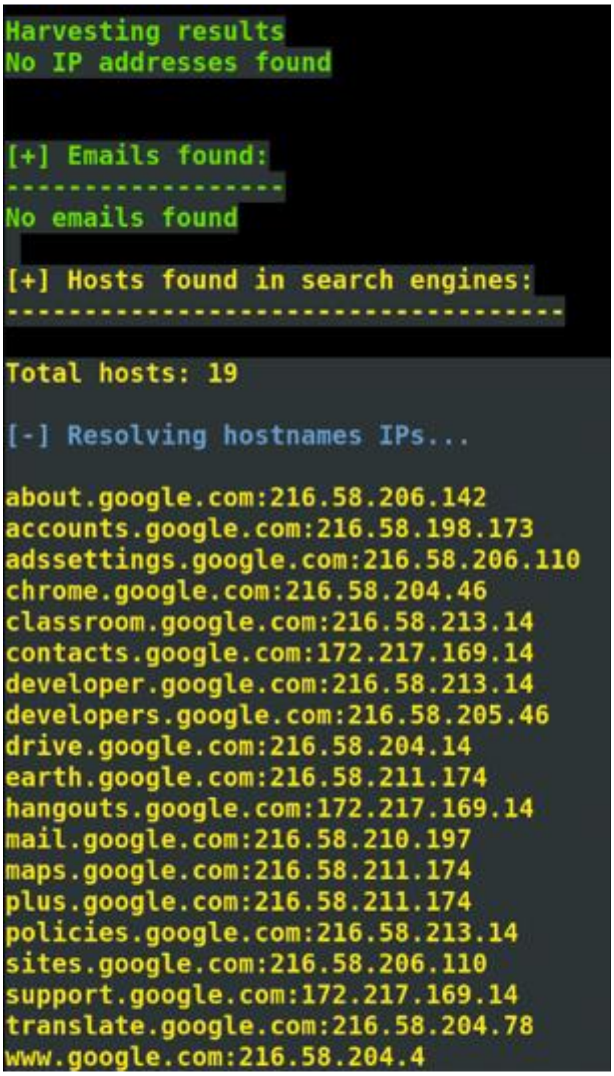
Some tools and services are mentioned in the below list.

1. The Harvester
2. Tweet Deck
3. Google Dorks
4. OSINT Framework
5. Reverse Image Searching (TinEye, Google)

The Harvester

The Harvester is an information gathering tool that utilizes OSINT sources to gather information about the target domain, and retrieve information such as hostnames, IP addresses, employees (and their positions), email addresses, and much more. The below screenshot shows performing simple reconnaissance on the domain Google.com, using Google as the data source:

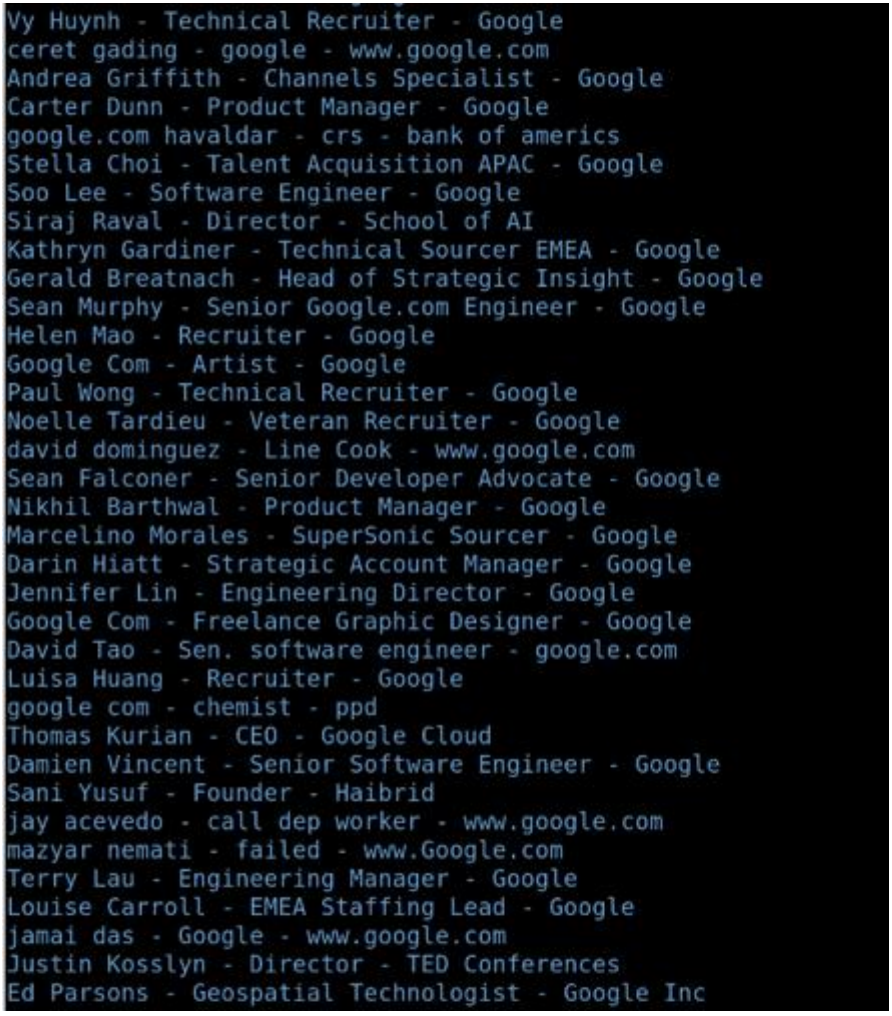
theharvester -d google.com -l 100 -b google
(tool) (target domain = google.com) (list 100 results max) (source = google)



```
Harvesting results
No IP addresses found


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
------------------------------------

Total hosts: 19

[-] Resolving hostnames IPs...

about.google.com:216.58.206.142
accounts.google.com:216.58.198.173
adssettings.google.com:216.58.206.110
chrome.google.com:216.58.204.46
classroom.google.com:216.58.213.14
contacts.google.com:172.217.169.14
developer.google.com:216.58.213.14
developers.google.com:216.58.205.46
drive.google.com:216.58.204.14
earth.google.com:216.58.211.174
hangouts.google.com:172.217.169.14
mail.google.com:216.58.210.197
maps.google.com:216.58.211.174
plus.google.com:216.58.211.174
policies.google.com:216.58.213.14
sites.google.com:216.58.206.110
support.google.com:172.217.169.14
translate.google.com:216.58.204.78
www.google.com:216.58.204.4
```

This didn't give us too much information, but knowing the IPs associated with google subdomains could be useful. Now let's try something a little bit different. If we wanted to launch social engineering attacks against some Google employees, we can quickly identify potential targets by setting the data source to be 'Linkedin' instead of 'Google':

theharvester -d google.com -l 100 -b linkedin
(tool) (target domain = google.com) (list 100 results max) (source = linkedin)



```
Vy Huynh - Technical Recruiter - Google
ceret gading - google - www.google.com
Andrea Griffith - Channels Specialist - Google
Carter Dunn - Product Manager - Google
google.com havaldar - crs - bank of americs
Stella Choi - Talent Acquisition APAC - Google
Soo Lee - Software Engineer - Google
Siraj Raval - Director - School of AI
Kathryn Gardiner - Technical Sourcer EMEA - Google
Gerald Breatnach - Head of Strategic Insight - Google
Sean Murphy - Senior Google.com Engineer - Google
Helen Mao - Recruiter - Google
Google Com - Artist - Google
Paul Wong - Technical Recruiter - Google
Noelle Tardieu - Veteran Recruiter - Google
david dominguez - Line Cook - www.google.com
Sean Falconer - Senior Developer Advocate - Google
Nikhil Barthwal - Product Manager - Google
Marcelino Morales - SuperSonic Sourcer - Google
Darin Hiatt - Strategic Account Manager - Google
Jennifer Lin - Engineering Director - Google
Google Com - Freelance Graphic Designer - Google
David Tao - Sen. software engineer - google.com
Luisa Huang - Recruiter - Google
google com - chemist - ppd
Thomas Kurian - CEO - Google Cloud
Damien Vincent - Senior Software Engineer - Google
Sani Yusuf - Founder - Haibrid
jay acevedo - call dep worker - www.google.com
mazyar nemati - failed - www.Google.com
Terry Lau - Engineering Manager - Google
Louise Carroll - EMEA Staffing Lead - Google
jamai das - Google - www.google.com
Justin Kosslyn - Director - TED Conferences
Ed Parsons - Geospatial Technologist - Google Inc
```

Now we have a list of potential targets, along with their job titles. We can do further reconnaissance on them using Linkedin itself and build up a profile on them using a tool like Maltego, then we can launch spear-phishing attacks as part of a threat simulation engagement!

Try using The Harvester with different domains, and different data sources. You can access the help sheet for this tool by using the command **theharvester** within the command-line. This will show you the available data sources, and other arguments to retrieve specific data.

TwitterDeck

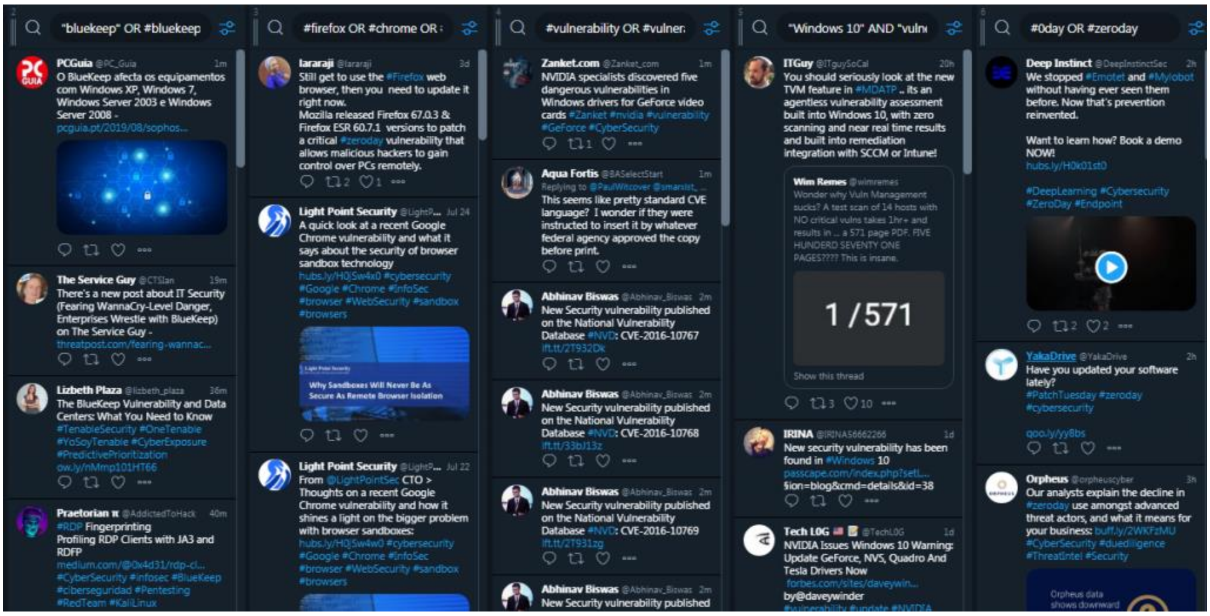
There are approximately 500 million tweets a day. That's a lot of information to get through, but TweetDeck makes it a lot easier to monitor trends, follow hashtags, and perform live searches. This is a useful tool for security professionals, as it allows us to monitor for events in real time, such as cyber-attacks, vulnerabilities being released, or even tracking malicious actor's activity.

As we're not going to be following or interacting with any accounts we're monitoring, you can use any Twitter account you want, so there's no real reason to use a throw-away or dummy account.

This is a section of a TweetDeck used to monitor for vulnerabilities affecting common software (such as browsers), major operation systems (in this case Windows 10), and threat actors.

From left to right, the columns are monitoring for the following activity:

1. **"bluekeep" OR #bluekeep OR cve-2019-0708**
   CVE-2019-0708, dubbed 'BlueKeep' was a Zero-Day vulnerability in Remote Desktop Protocol (RDP) that could allow an unauthenticated, remote attacker to bypass authentication.
2. **#firefox OR #chrome OR #internetexplorer OR #IE**
   Following vulnerabilities in Firefox, Chrome, and Internet Explorer.
3. **#vulnerability OR #vulnerabilities OR #CVE**
   Broad search term for vulnerabilities (does bring back a lot of non-security tweets due to common language).
4. **"Windows 10" and "vulnerability"**
   Monitoring for Windows 10 vulnerabilities.
5. **#0day OR #zeroday**
   Monitoring for zero-day vulnerabilities that are publicly announced on Twitter.



"bluekeep" OR #bluekeep

PCGuia @PC_Guia 1m
O BlueKeep afecta os equipamentos com Windows XP, Windows 7, Windows Server 2003 e Windows Server 2008 - pcguia.pt/2019/08/sophos...

The Service Guy @CTSlan 19m
There's a new post about IT Security (Fearing WannaCry-Level Danger, Enterprises Wrestle with BlueKeep) on The Service Guy - threatpost.com/fearing-wannac...

Lizbeth Plaza @lizbeth_plaza 36m
The BlueKeep Vulnerability and Data Centers: What You Need to Know #TenableSecurity #OneTenable #YoSoyTenable #CyberExposure #PredictivePrioritization ow.ly/nMmp101HT66

Praetorian π @AddictedToHack 40m
#RDP Fingerprinting
Profiling RDP Clients with JA3 and RDFP
medium.com/@0x4d31/rdp-cl...
#CyberSecurity #infosec #BlueKeep #ciberseguridad #Pentesting #RedTeam #KaliLinux

#firefox OR #chrome OR

lararaji @lararaji 3d
Still get to use the #Firefox web browser, then you need to update it right now.
Mozilla released Firefox 67.0.3 & Firefox ESR 60.7.1 versions to patch a critical #zeroday vulnerability that allows malicious hackers to gain control over PCs remotely.
2 1

Light Point Security @LightP... Jul 24
A quick look at a recent Google Chrome vulnerability and what it says about the security of browser sandbox technology
hubs.ly/H0jSw4x0 #cybersecurity #Google #Chrome #InfoSec #browser #WebSecurity #sandbox #browsers

Light Point Security
Why Sandboxes Will Never Be As Secure As Remote Browser Isolation

Light Point Security @LightP... Jul 22
From @LightPointSec CTO > Thoughts on a recent Google Chrome vulnerability and how it shines a light on the bigger problem with browser sandboxes:
hubs.ly/H0jSw4w0 #cybersecurity #Google #Chrome #InfoSec #browser #WebSecurity #sandbox #browsers

#vulnerability OR #vulner

Zanket.com @Zanket_com 1m
NVIDIA specialists discovered five dangerous vulnerabilities in Windows drivers for GeForce video cards #Zanket #nvidia #vulnerability #GeForce #CyberSecurity
1

Aqua Fortis @BASelectStart 1m
Replying to @PaulWitcover @smarsist_ ...
This seems like pretty standard CVE language? I wonder if they were instructed to insert it by whatever federal agency approved the copy before print.

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10767 ift.tt/2T932Dk

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10768 ift.tt/33bJ13z

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10769 ift.tt/2T931zg

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published

"Windows 10" AND "vuln

ITGuy @ITguySoCal 20h
You should seriously look at the new TVM feature in #MDATP .. its an agentless vulnerability assessment built into Windows 10, with zero scanning and near real time results and built into remediation integration with SCCM or Intune!

Wim Remes @wimremes
Wonder why Vuln Management sucks? A test scan of 14 hosts with NO critical vulns takes 1hr+ and results in ... a 571 page PDF. FIVE HUNDERD SEVENTY ONE PAGES???? This is insane.
1 / 571
Show this thread
3 10

IRINA @IRINA56662266 1d
New security vulnerability has been found in #Windows 10
passcape.com/index.php?setl... $ion=blog&cmd=details&id=38

Tech LOG 🇺🇸 📝 @TechLOG 1d
NVIDIA Issues Windows 10 Warning: Update GeForce, NVS, Quadro And Tesla Drivers Now
forbes.com/sites/daveywin...
by@daveywinder
#vulnerability #update #NVIDIA

#0day OR #zeroday

Deep Instinct @DeepInstinctSec 2h
We stopped #Emotet and #Mylobot without having ever seen them before. Now that's prevention reinvented.

Want to learn how? Book a demo NOW!
hubs.ly/H0k01st0

#DeepLearning #Cybersecurity #ZeroDay #Endpoint
2 2

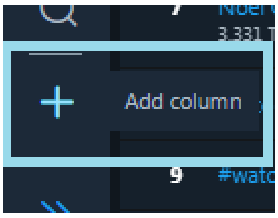
YakaDrive @YakaDrive 2h
Have you updated your software lately?
#PatchTuesday #zeroday #cybersecurity

goo.ly/yy8bs

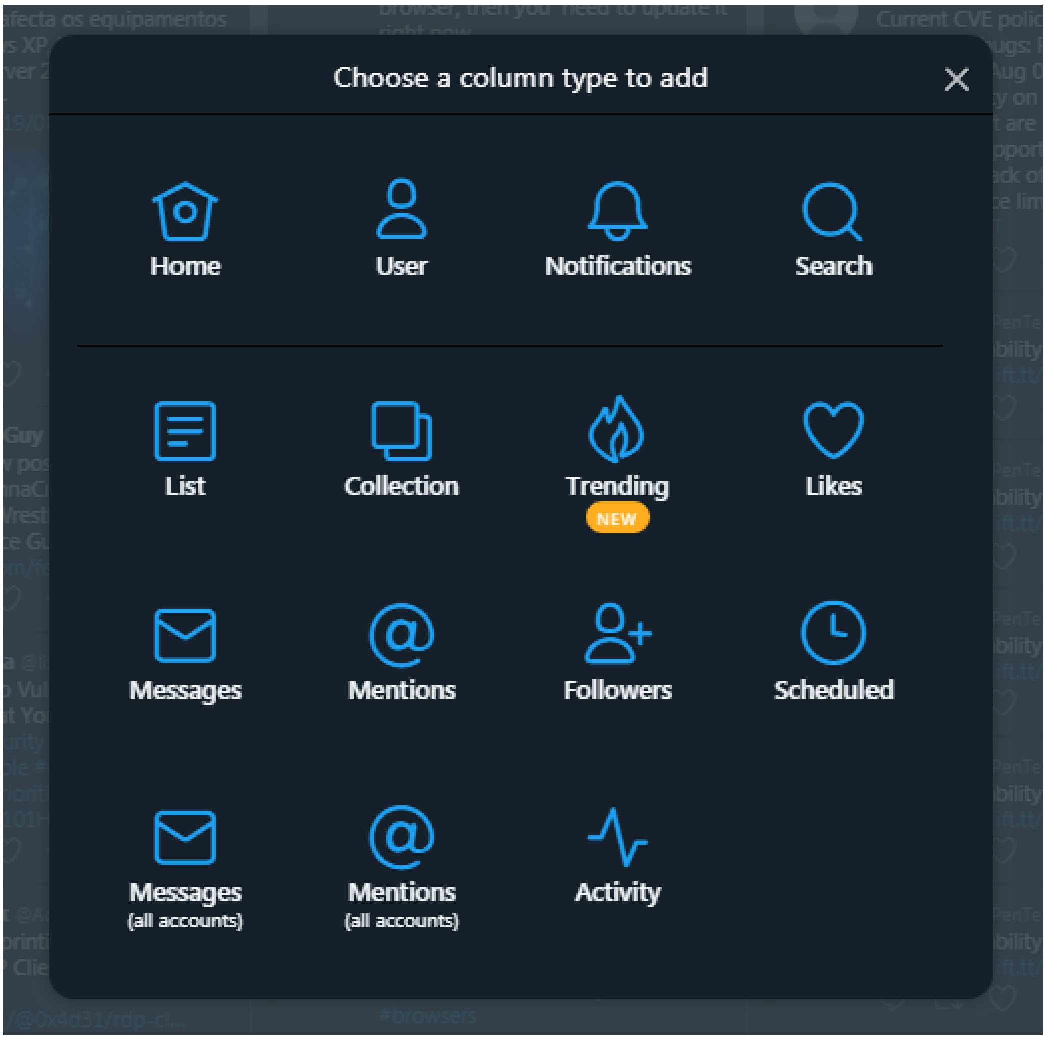
Orpheus @orpheuscyber 3h
Our analysts explain the decline in #zeroday use amongst advanced threat actors, and what it means for your business: buff.ly/2WKFzMU #CyberSecurity #duediligence #ThreatIntel #Security

Orpheus data shows downward

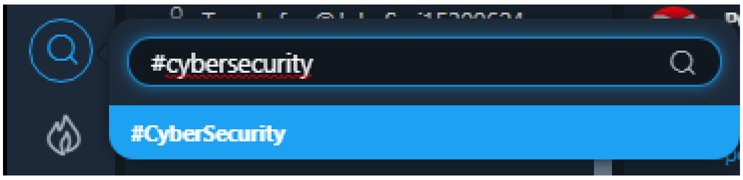
To add a search column, click on the "+" icon on the left-hand side.



A pop-up will allow us to choose what type of column we want to add to our Deck. In this case, we're going to be using the "Search" column type, in the top right.

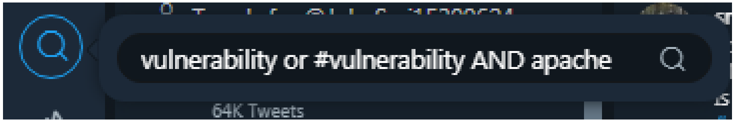


This gives us a blank column, where we can enter in our own search queries. A quick example would be monitoring for tweets using the hashtag "#cybersecurity".



We can start to build out these searches to look for a specific activity. In the example below, we are looking for the following:

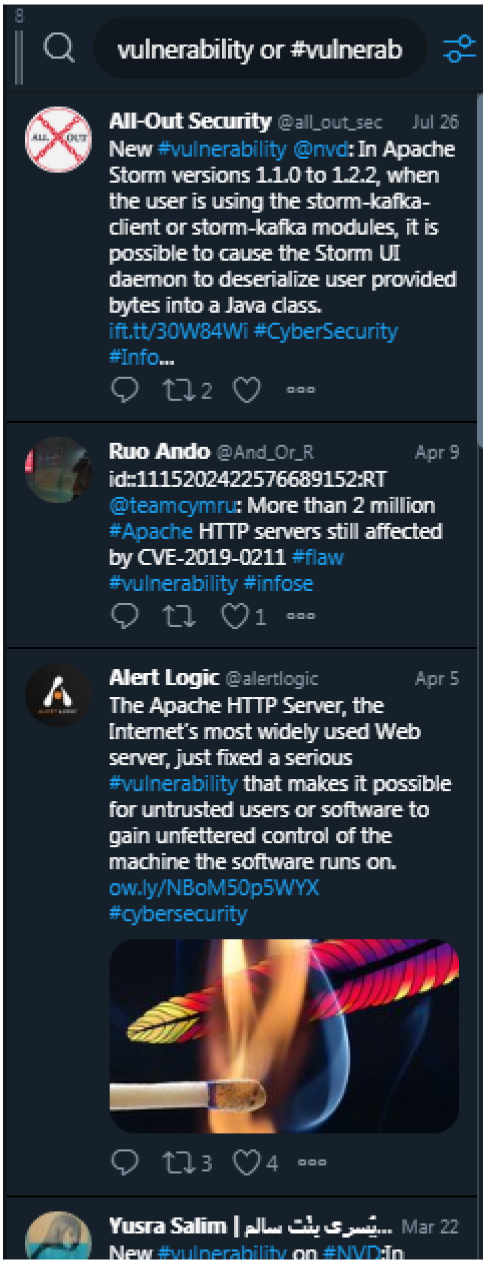
- Mention of the string “vulnerability” AND the string “apache”
- OR the hashtag “#vulnerability” AND the string “apache”
- This will show us tweets such as “*Wow – just discovered a new vulnerability in apache, can’t wait to exploit it!*“, or “*CRITICAL #VULNERABILITY announced in apache v1.5 – Patch your systems now!*“



vulnerability or #vulnerability AND apache

64K Tweets

This is what the column will look like once we’ve created it. As we can see, these tweets all have “vulnerability” or “#vulnerability” AND “apache”.



vulnerability or #vulnerab

All-Out Security @all_out_sec Jul 26

New #vulnerability @nvd: In Apache Storm versions 1.1.0 to 1.2.2, when the user is using the storm-kafka-client or storm-kafka modules, it is possible to cause the Storm UI daemon to deserialize user provided bytes into a Java class. ift.tt/30W84Wi #CyberSecurity #Info...

Ruo Ando @And_Or_R Apr 9

id::1115202422576689152:RT @teamcymru: More than 2 million #Apache HTTP servers still affected by CVE-2019-0211 #flaw #vulnerability #infose

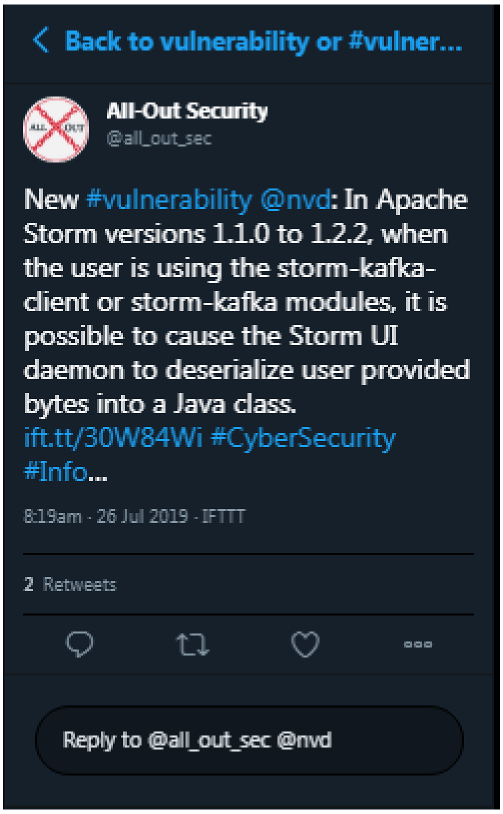
Alert Logic @alertlogic Apr 5

The Apache HTTP Server, the Internet’s most widely used Web server, just fixed a serious #vulnerability that makes it possible for untrusted users or software to gain unfettered control of the machine the software runs on. ow.ly/NBoM50p5WYX #cybersecurity

Yusra Salim | يسرى بنت سالم... Mar 22

New #vulnerability on #NVD:In

We can then click on these Tweets to see them individually, allowing us to comment, like, or retweet if we wanted to!



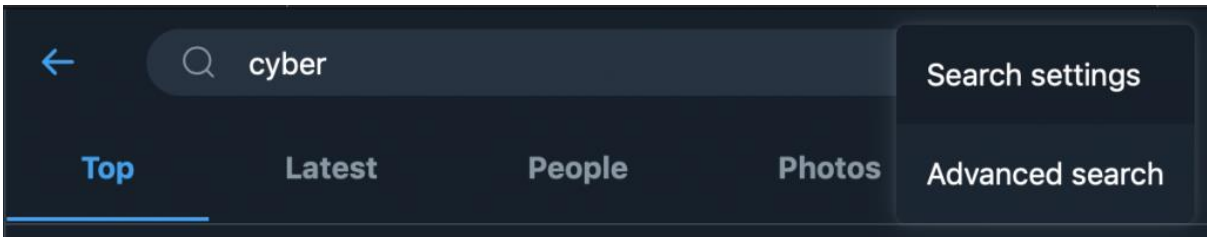
All-Out Security
@all_out_sec

New #vulnerability @nvd: In Apache Storm versions 1.1.0 to 1.2.2, when the user is using the storm-kafka-client or storm-kafka modules, it is possible to cause the Storm UI daemon to deserialize user provided bytes into a Java class. ift.tt/30W84Wi #CyberSecurity #Info...

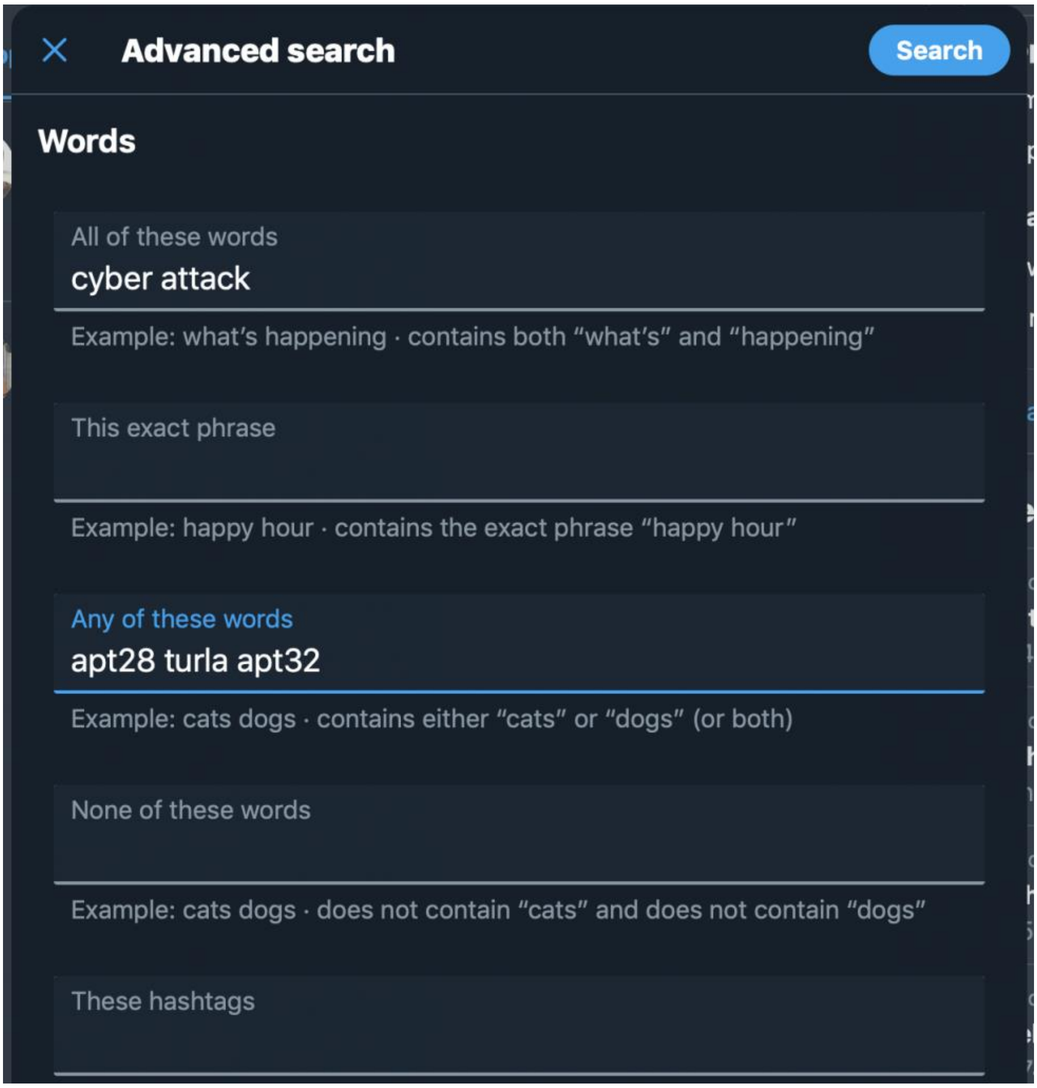
8:19am · 26 Jul 2019 · IFTTT

2 Retweets

We can create our search queries in Twitter’s platform, by using their Advanced Search tools. To get to these, open up Twitter, search for anything in the search bar, click the ⚙ icon, and choose “Advanced Search”.



From here, we’re able to create complex search queries. In this example, we are looking for the strings “cyber” and “attack”, and the tweet must also contain one of the following; “apt28”, “turla”, or “apt32” (well-known threat actors).



Words

All of these words
cyber attack

Example: what's happening · contains both "what's" and "happening"

This exact phrase

Example: happy hour · contains the exact phrase "happy hour"

Any of these words
apt28 turla apt32

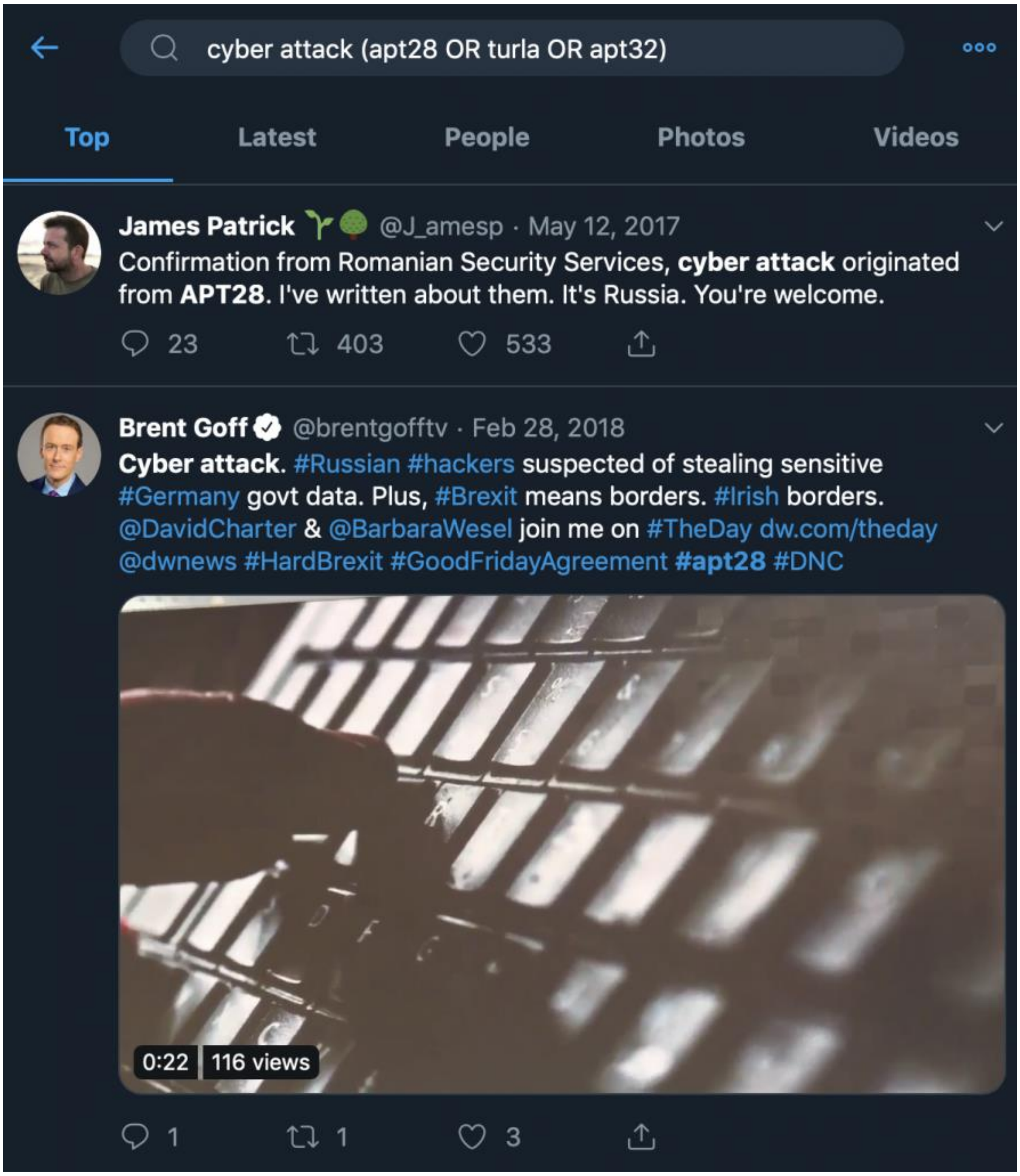
Example: cats dogs · contains either "cats" or "dogs" (or both)

None of these words

Example: cats dogs · does not contain "cats" and does not contain "dogs"

These hashtags

As we can see in the first two tweets, they both mention the terms "cyber attack" and "apt28". We can now copy and paste this search string into our TweetDeck, allowing us to continually monitor for this specific activity.



James Patrick @J_amesp · May 12, 2017
Confirmation from Romanian Security Services, **cyber attack** originated from **APT28**. I've written about them. It's Russia. You're welcome.

Brent Goff @brentgofftv · Feb 28, 2018
Cyber attack. #Russian #hackers suspected of stealing sensitive #Germany govt data. Plus, #Brexit means borders. #Irish borders. @DavidCharter & @BarbaraWesel join me on #TheDay dw.com/theday @dwnews #HardBrexit #GoodFridayAgreement **#apt28** #DNC

And there you have it! A quick walkthrough of TweetDeck, and using it as a monitoring platform. It doesn't just have to be cyber-attacks or vulnerabilities, it can also be used to track geopolitical news, terror attacks, specific accounts, and anything else you may want to follow.

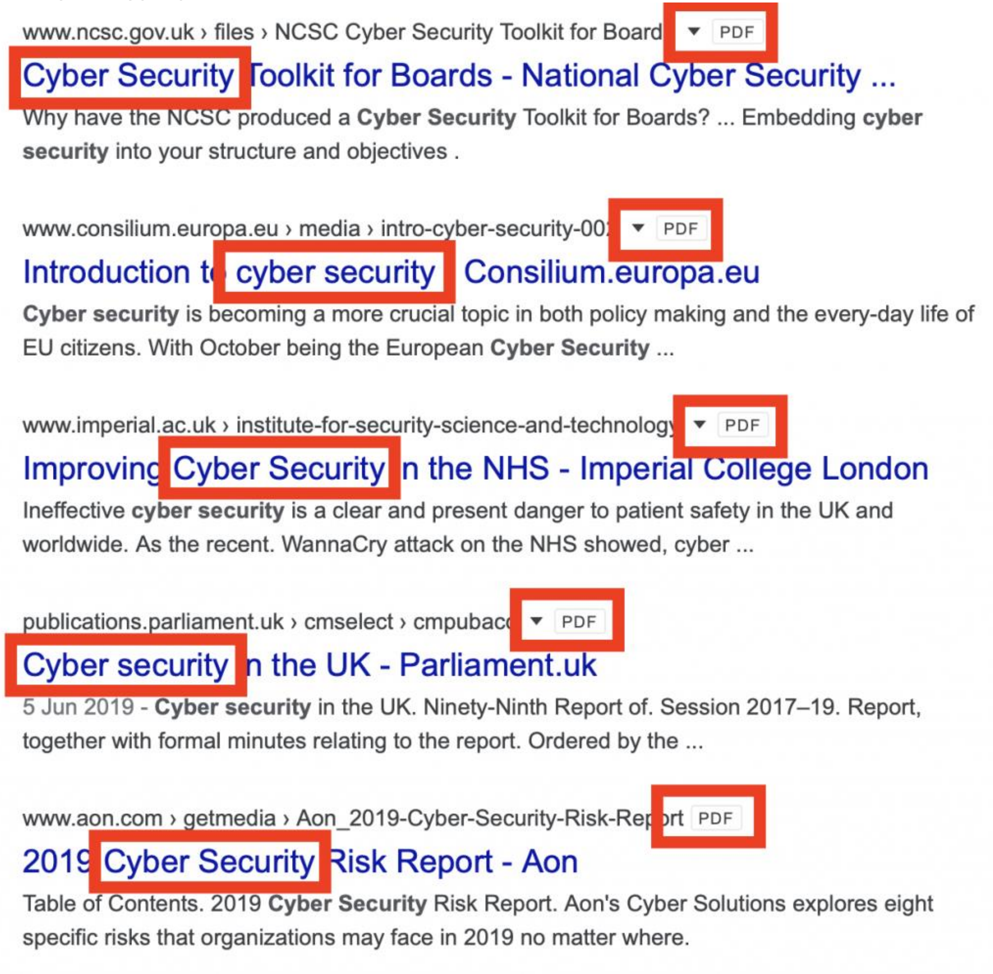
Google Dorks

Google is helpful in general, but Google Dorks are search hacks where we can use special arguments in a normal Google query to find specific information. Dorks come in the format **operator:keyword**, an example of this would be **filetype:pdf**. Real-world examples of using Dorks include:

- **Retrieving files from domains.**
- **Finding hidden webpages and login portals.**
- **Subdomain enumeration**.

Finding Files

Let's start of by seeing what PDFs we can find that are associated with cyber security, using the dork query:
Cyber Security filetype:pdf.



www.ncsc.gov.uk › files › NCSC Cyber Security Toolkit for Board ▾ PDF
Cyber Security Toolkit for Boards - National Cyber Security ...
Why have the NCSC produced a **Cyber Security** Toolkit for Boards? ... Embedding **cyber security** into your structure and objectives .

www.consilium.europa.eu › media › intro-cyber-security-00 ▾ PDF
Introduction t cyber security Consilium.europa.eu
Cyber security is becoming a more crucial topic in both policy making and the every-day life of EU citizens. With October being the European **Cyber Security** ...

www.imperial.ac.uk › institute-for-security-science-and-technolog ▾ PDF
Improvin Cyber Security n the NHS - Imperial College London
Ineffective **cyber security** is a clear and present danger to patient safety in the UK and worldwide. As the recent. WannaCry attack on the NHS showed, cyber ...

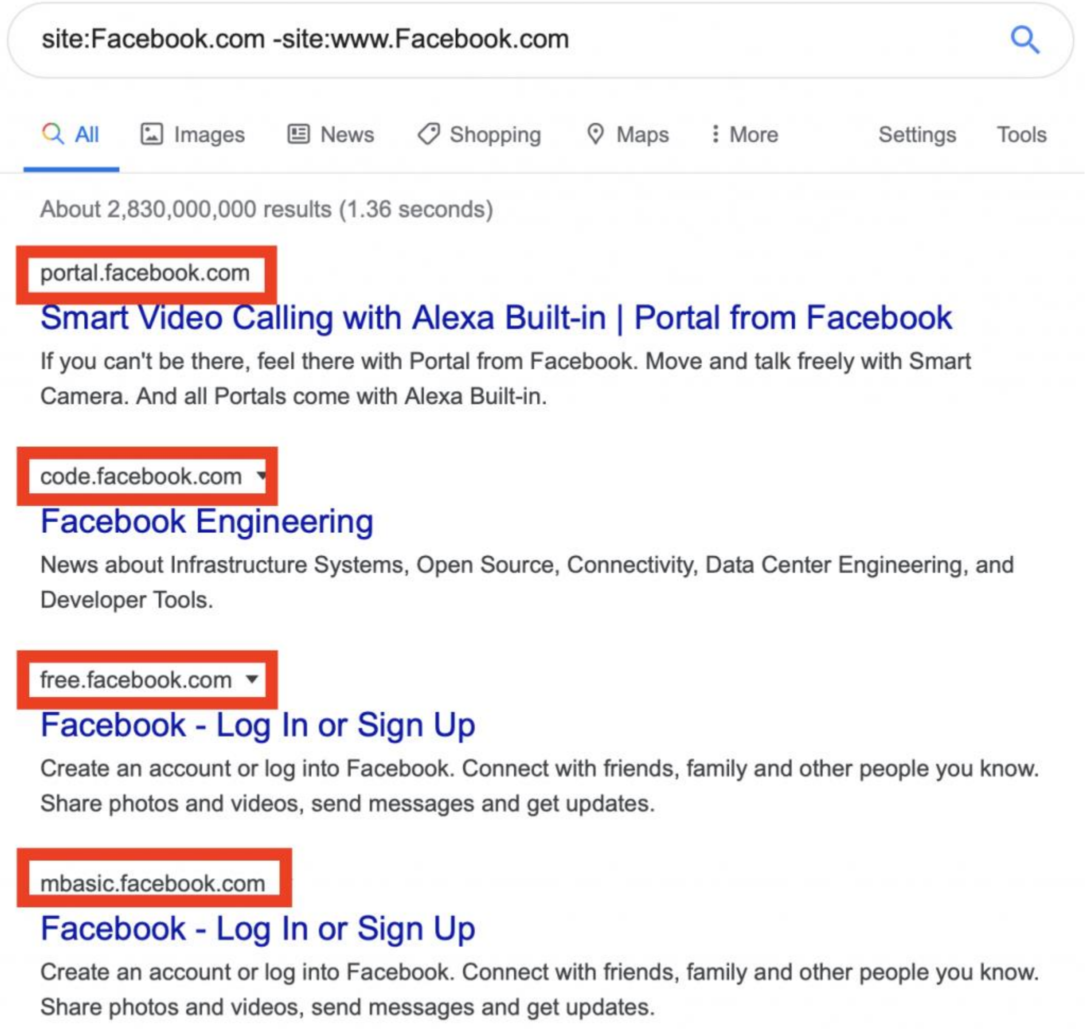
publications.parliament.uk › cmselect › cmpubac ▾ PDF
Cyber security n the UK - Parliament.uk
5 Jun 2019 - **Cyber security** in the UK. Ninety-Ninth Report of. Session 2017–19. Report, together with formal minutes relating to the report. Ordered by the ...

www.aon.com › getmedia › Aon_2019-Cyber-Security-Risk-Re rt PDF
201 Cyber Security Risk Report - Aon
Table of Contents. 2019 **Cyber Security** Risk Report. Aon's Cyber Solutions explores eight specific risks that organizations may face in 2019 no matter where.

In the above screenshot we can see that the search has brought back any PDF files that contain the strings "cyber" and "security. We can use this to see what files a company is hosting online, and see if any are confidential and should not be publicly-accessible. It is also possible to retrieve information about internal systems and users by looking at the metadata of files to see when they were created and who by. Documents can also be used to create custom wordlists for password attacks against specific organisations. Try this yourself with a search term or a domain (such as Facebook.com filetype:pdf).

Subdomain Enumeration

Now let’s see how Dorks can be used to enumerate all subdomains of a domain, for passive reconnaissance purposes. For this, we will use Facebook again as the example, with the following query:
site:Facebook.com -site:www.Facebook.com
(Look for sites that include .Facebook.com) (but NOT www.Facebook.com)


site:Facebook.com -site:www.Facebook.com

About 2,830,000,000 results (1.36 seconds)

portal.facebook.com
Smart Video Calling with Alexa Built-in | Portal from Facebook
If you can't be there, feel there with Portal from Facebook. Move and talk freely with Smart Camera. And all Portals come with Alexa Built-in.

code.facebook.com
Facebook Engineering
News about Infrastructure Systems, Open Source, Connectivity, Data Center Engineering, and Developer Tools.

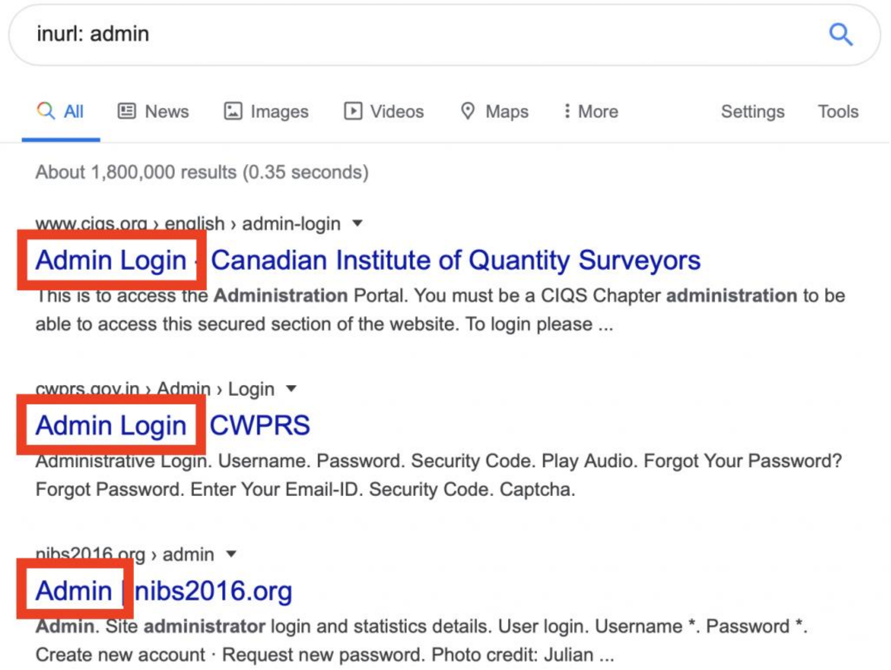
free.facebook.com
Facebook - Log In or Sign Up
Create an account or log into Facebook. Connect with friends, family and other people you know. Share photos and videos, send messages and get updates.

mbasic.facebook.com
Facebook - Log In or Sign Up
Create an account or log into Facebook. Connect with friends, family and other people you know. Share photos and videos, send messages and get updates.

Here we can see the list begins with two subdomains, portal.facebook.com, and code.facebook.com. We have successfully enumerated subdomains using Google Dorks. This is a great method for identifying uncommon webpages that may feature a login portal or valuable information such as development environments, files, and more.

Keyword Searching

Using the Dork **inurl: (value)** we can look for specific keywords in a much more refined way than normal google searches. Using the query **inurl: admin** we can see a number of what appears to be admin login portals. This would be great if we were working as an attacker (if in scope, we can brute force or bypass the login portal to access administrator dashboards) or a defender (we can work to secure these portals so they are not compromised).



About 1,800,000 results (0.35 seconds)

www.ciqs.org › english › admin-login ▾

Admin Login - Canadian Institute of Quantity Surveyors

This is to access the **Administration** Portal. You must be a CIQS Chapter **administration** to be able to access this secured section of the website. To login please ...

cwprs.gov.in › Admin › Login ▾

Admin Login CWPRS

Administrative Login. Username. Password. Security Code. Play Audio. Forgot Your Password? Forgot Password. Enter Your Email-ID. Security Code. Captcha.

nibs2016.org › admin ▾

Admin | nibs2016.org

Admin. Site **administrator** login and statistics details. User login. Username *. Password *. Create new account · Request new password. Photo credit: Julian ...

OSINT Framework

This website is a hub for **hundreds** of OSINT sources and tools, and is easily sorted so you can find the tool that you need quickly. You can access the site here – https://osintframework.com

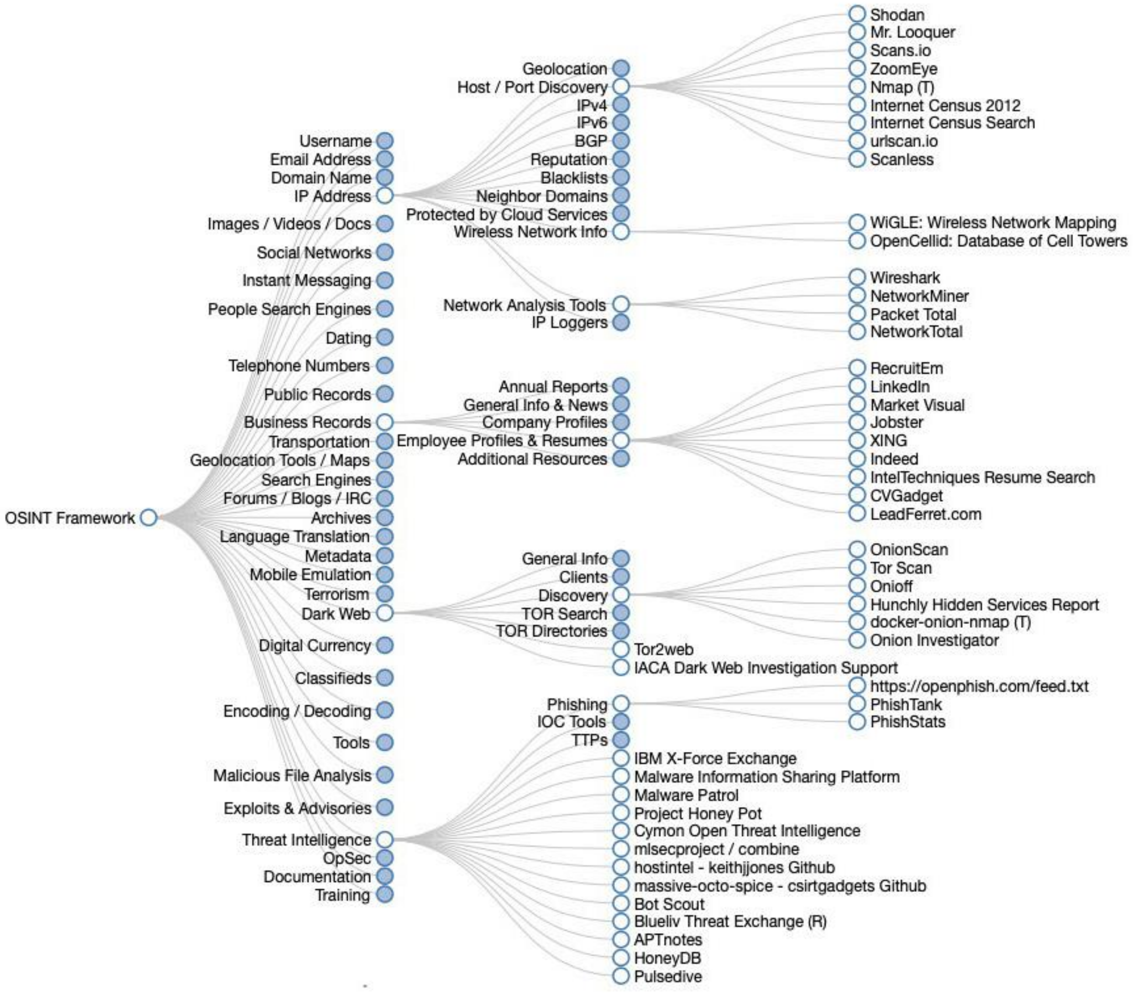
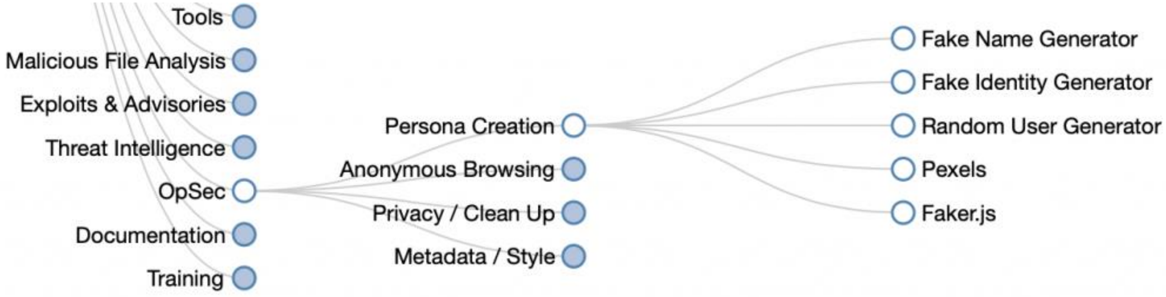


Image from https://osintframework.com/

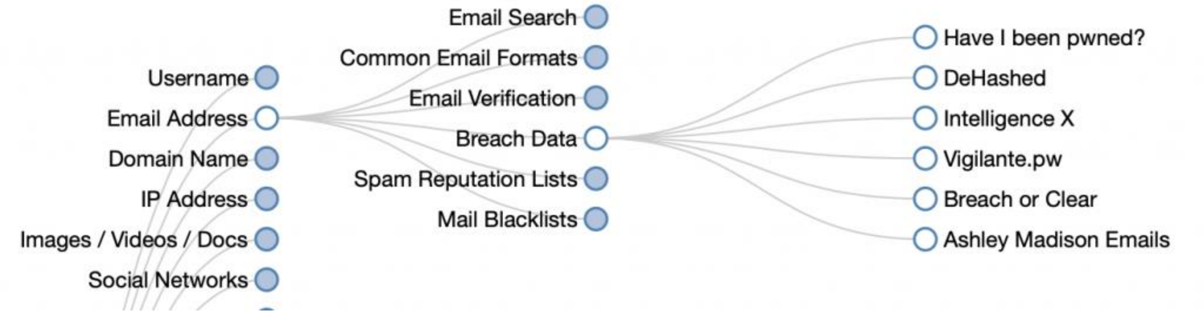
Use Case: Social Engineering Attacks

Say we wanted to create a fake persona so we could launch some social-engineering attacks during a red team engagement at our company. By opening the **OpSec** arm, and then **Persona Creation**, we are provided with 5 links to online tools that can help us with the task we are trying to complete. This can help us build a rich and more authentic profile, than if we were just filling out details off the top of our head.



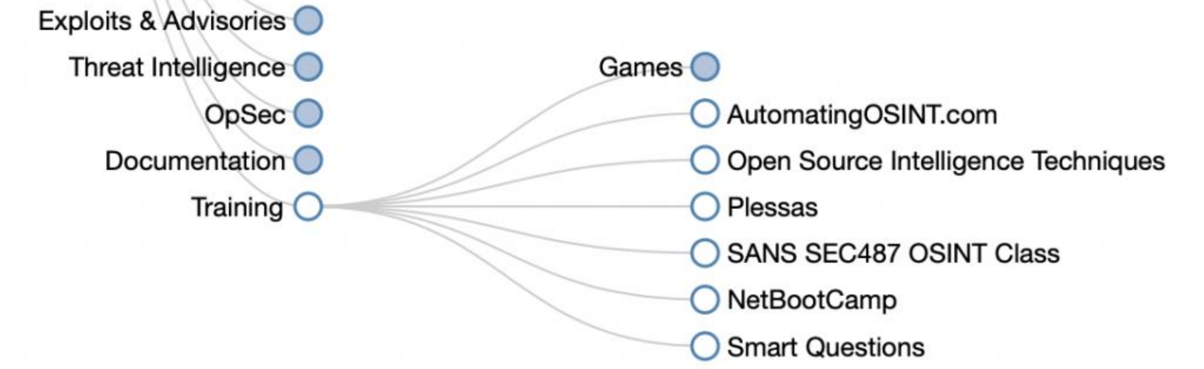
Use Case: Are Target Emails Compromised?

Without diving down the rabbit-hole that is Threat Intelligence, we can quickly get a sense of whether a target email address has been mentioned in a data breach. Why is this useful? Because if we get an indication it has been leaked before, we can then start to explore paths such as finding data breach dumps on the dark web, and seeing if the email address has been linked with any passwords – then we can use these for password or social-engineering attacks. If we visit the **Email Address** branch, then the **Data Breach** sub-branch, we are provided with several online services that allow us to enter email addresses in, to see if they have been breached.



Use Case: Boosting OSINT Skills And Knowledge

OSINT Framework offers a good selection of OSINT training resources, so if you're looking to further your skills then check these out. These are available under the **Training** branch.



We strongly suggest you check out this tool and see what interesting sites and tools you can find from it. https://www.osintframework.com

Reverse Image Searching

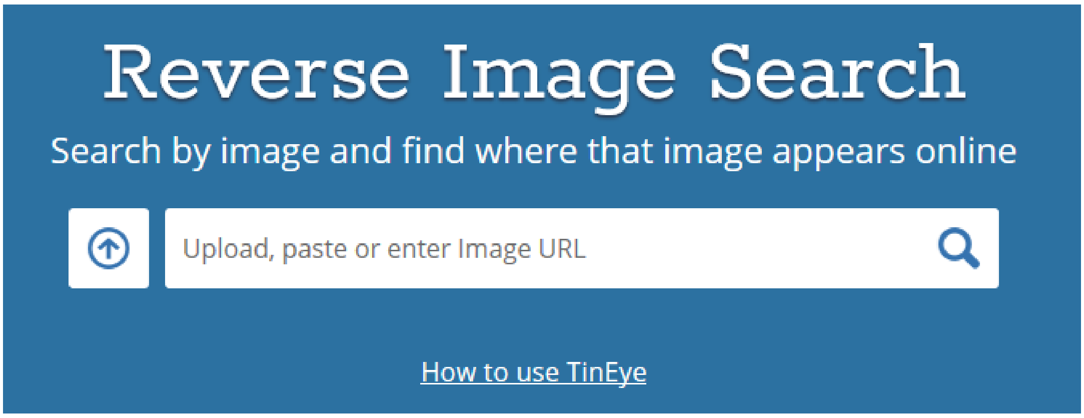
1. TinEye

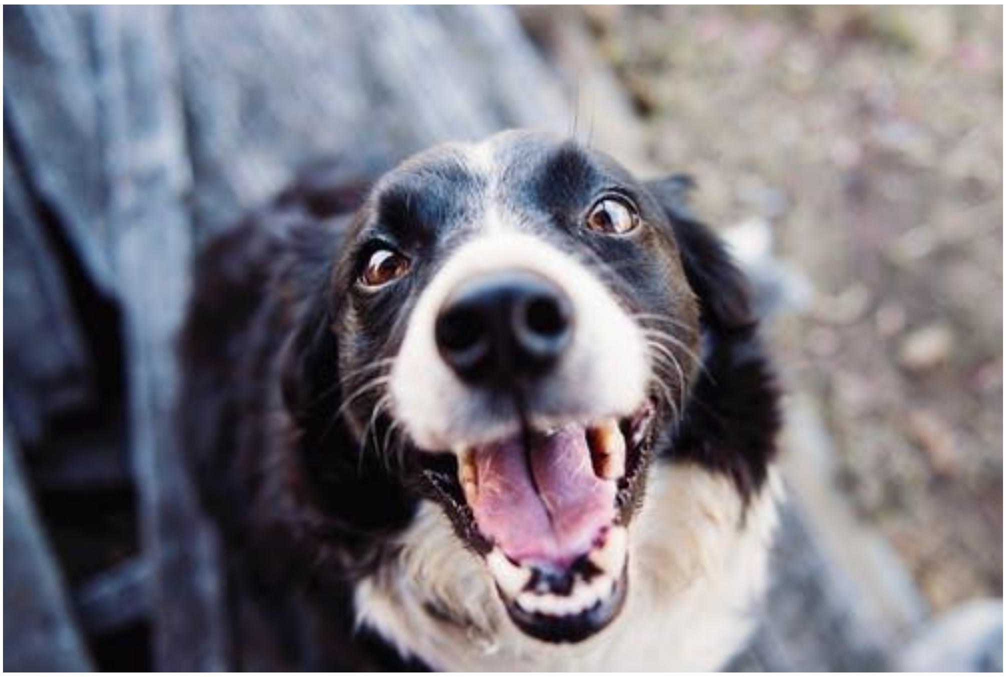
TinEye is an image search and recognition company, which offers customers the ability to receive alerts when their images are identified on the internet. This could be useful for Security Blue Team, as if people started posting our logo, it could potentially be someone pretending to be us, using our branding to give them more authenticity. This could also be useful for photographers who don't want their images shared without proper authorization.

Moving away from the Alerts service they offer, anyone can use TinEye to conduct reverse image searches, which is where we upload an image, and see where else it is present on the internet. We'll cover how to use it, and provide a couple of use cases for using this tool.

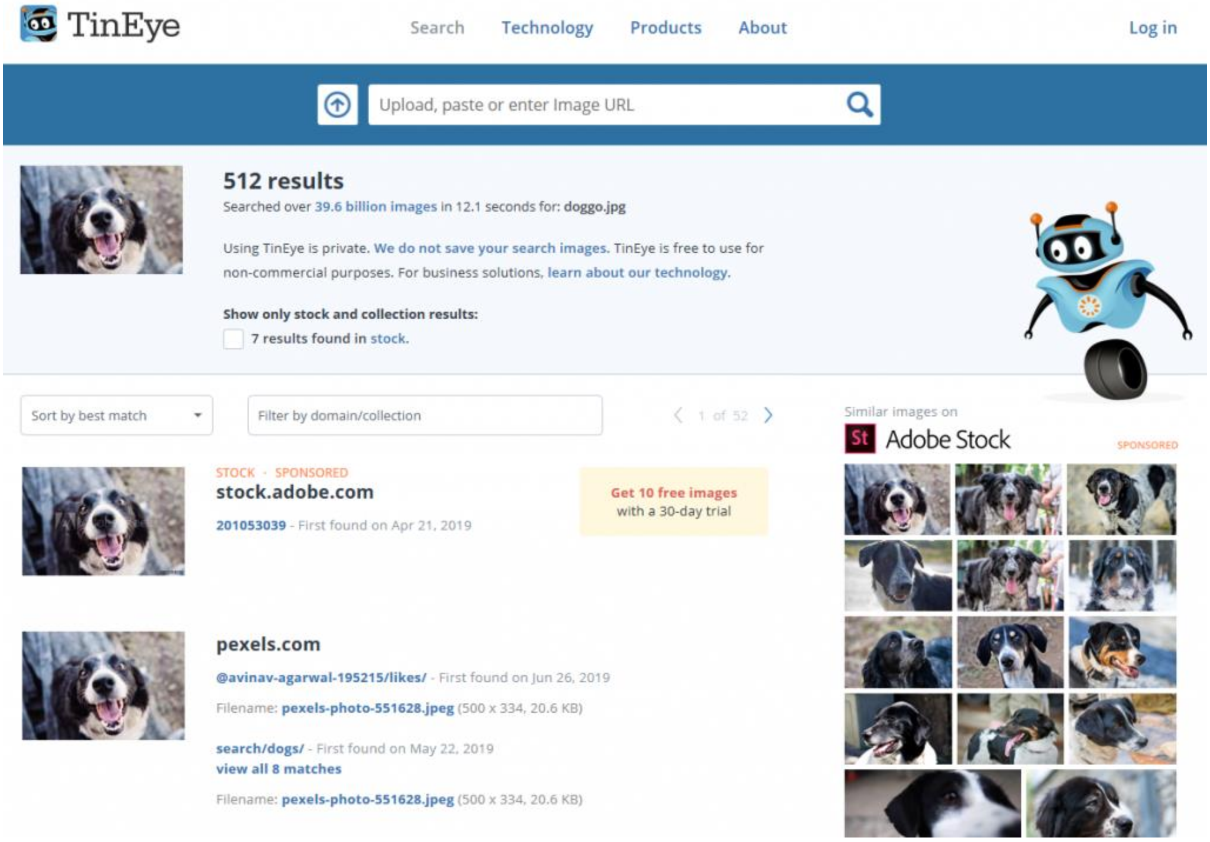
Using TinEye

Head over to https://tineye.com/ and you'll see the below search bar at the top of the page. You have the option of uploading an image or using a URL that takes you to a hosted image. For this example, we'll use the upload feature with the below stock image of a dog. We should expect to see a lot of results for this image, as it will likely be used across the internet due to its nature.


Reverse Image Search
Search by image and find where that image appears online
Upload, paste or enter Image URL
How to use TinEye



After the search was completed, we were presented with the below screen, which shows that this exact image was found in **512 different places**, amongst the **total 39.6 billion images** that were processed in an incredible **12.1 seconds**.



TinEye
Search
Technology
Products
About
Log in
Upload, paste or enter Image URL
Sort by best match
Filter by domain/collection
1 of 52
Get 10 free images with a 30-day trial

512 results

Searched over 39.6 billion images in 12.1 seconds for: doggo.jpg

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, learn about our technology.

Show only stock and collection results:

□ 7 results found in stock.

Similar images on St Adobe Stock SPONSORED

STOCK · SPONSORED

stock.adobe.com

201053039 - First found on Apr 21, 2019

pexels.com

@avinav-agarwal-195215/likes/ - First found on Jun 26, 2019

Filename: pexels-photo-551628.jpeg (500 x 334, 20.6 KB)

search/dogs/ - First found on May 22, 2019

view all 8 matches

Filename: pexels-photo-551628.jpeg (500 x 334, 20.6 KB)

Use Case: Identifying Social-Media Fakes

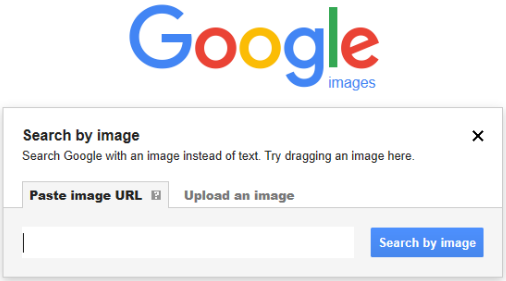
When people create fake social-media accounts, likely, they're not using a unique photo. Chances are they've to google something along the lines of "profile photo generator" and used one of them. These are usually really easy to identify just by looking at them (no one smiles *that* much), however, using TinEye we can quickly identify fakes by seeing how common the profile photo is. We should expect to see anywhere between 0-10 results, depending on how much the photo subject loves using that specific photo. If we reverse search a profile picture and it has hundreds of thousands of hits, this should immediately throw red flags. We can then start to look at the websites the image features on (we can see this on the screenshot above). If we see stock photo sites or similar, we know that it's pretty likely this is a fake account, using someone else's photo. This doesn't just apply to profile pictures – if an account is posting some pretty generic photos, we can also check how common they are. Two people can't take the exact some photo unintentionally, so if their images have even a low number of hits, this could be classed as suspicious.

Use Case: Brand Reputation Monitoring

Whilst there are better ways to do this, using the TinEye Alerts service, you can be notified every time one of your images is identified on the internet. This can be useful for monitoring the use of logos, especially trademarked ones.

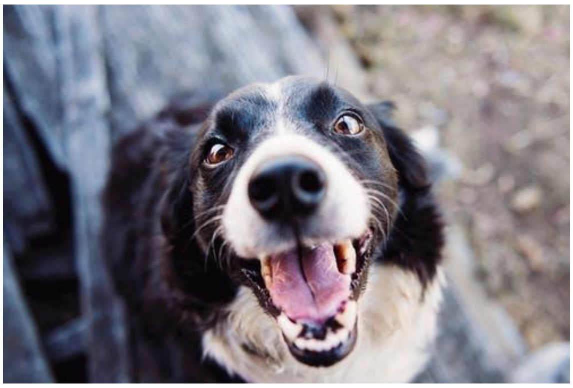
2. Google Image Search

Google Image Search is very similar to TinEye as they share the core functionality. Simply head over to https://images.google.com and you're able to search for an image URL, or upload an image manually. Let's try using the dog stock photo from the TinEye lesson.

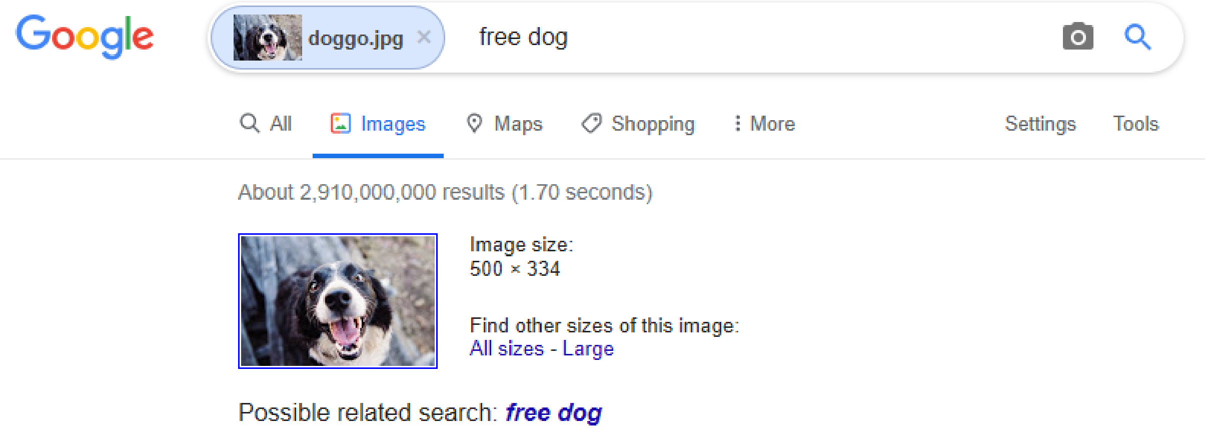


Search by image

Search Google with an image instead of text. Try dragging an image here.



In the below screenshots we can see that Google provided us with some interesting results based on the image we uploaded (above). At the top of the page (left screenshot), we can see the image in the search bar. There is also the phrase "free dog" which was generated by Google after analyzing the image, webpages where it is present, and any keywords that are commonly used in an attempt to describe what content the image contains. Google has searched any indexed pages for the image we uploaded, which has returned 2,910,000,000 results. Scrolling down the results page (right screenshot) we can see that Google is showing us any pages that include complete matches of the image we searched for.

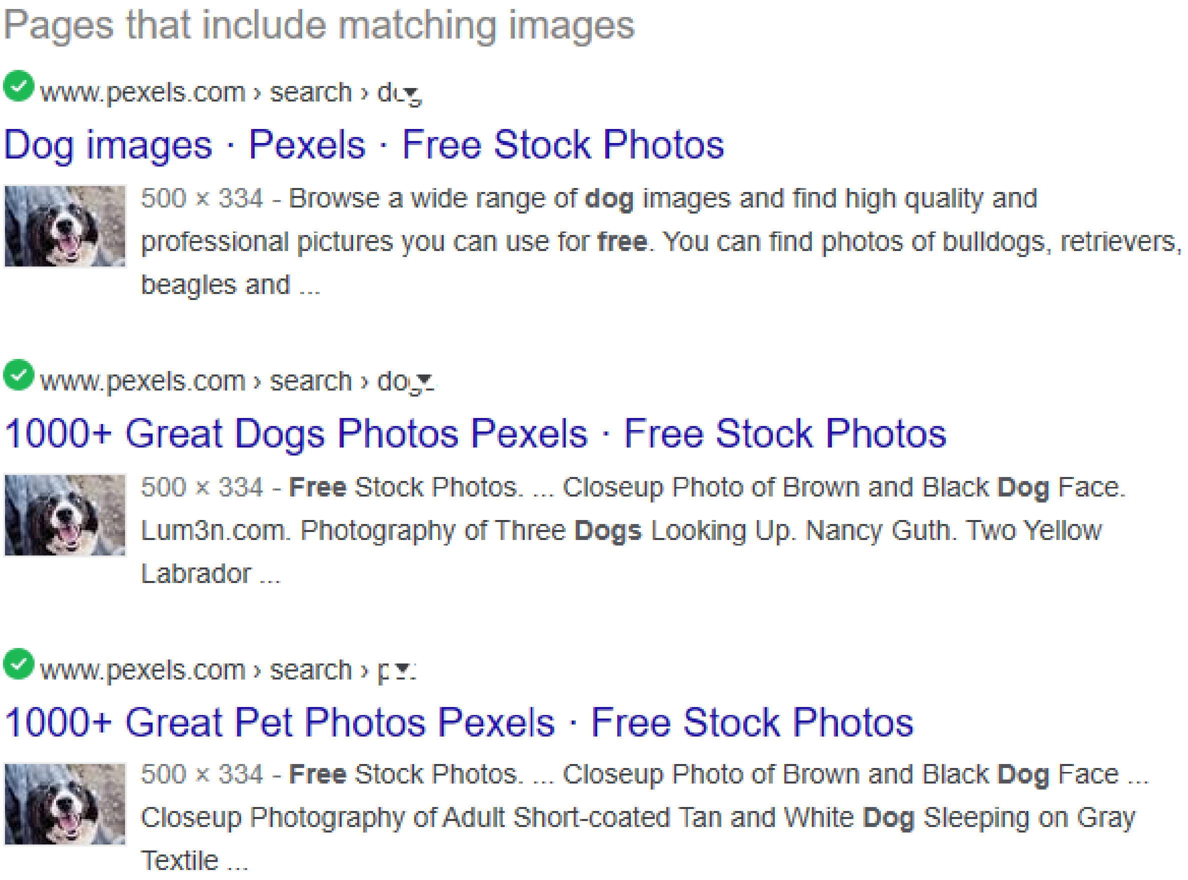


About 2,910,000,000 results (1.70 seconds)

Image size:
500 × 334

Find other sizes of this image:
All sizes - Large

Possible related search: ***free dog***



Pages that include matching images

www.pexels.com › search › d

Dog images · Pexels · Free Stock Photos

500 × 334 - Browse a wide range of **dog** images and find high quality and professional pictures you can use for **free**. You can find photos of bulldogs, retrievers, beagles and ...

www.pexels.com › search › do

1000+ Great Dogs Photos Pexels · Free Stock Photos

500 × 334 - **Free** Stock Photos. ... Closeup Photo of Brown and Black **Dog** Face. Lum3n.com. Photography of Three **Dogs** Looking Up. Nancy Guth. Two Yellow Labrador ...

www.pexels.com › search › p

1000+ Great Pet Photos Pexels · Free Stock Photos

500 × 334 - **Free** Stock Photos. ... Closeup Photo of Brown and Black **Dog** Face ... Closeup Photography of Adult Short-coated Tan and White **Dog** Sleeping on Gray Textile ...

Wayback Machine (https://archive.org/web/)

"Have you ever thought of taking notes/archiving websites that may not be available someday or Just keep snap of the browser view of your favorite webpage and be available to you any time?"

Then Wayback Machine is your answer. It is a non-profit digital library of internet sites. It is very handy in taking screenshots. These also help in archiving Twitter Tweets. All you need is the tweet's URL, and you can view the tweet as it is in the future.

"The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form."

This library of screenshots becomes a powerful tool in performing OSINT. These screenshots by random people sometimes help get unique information regarding the Webpage/Account.

Is OSINT illegal?

While OSINT techniques are often used by malicious hackers as reconnaissance before they launch an illegal attack, for the most part, the tools and techniques themselves are perfectly legal—after all, they're designed to help you home in on data that's published or otherwise in the public view. Even government agencies are encouraged to use OSINT techniques to ferret out holes in their cybersecurity defenses.