

WannaCry & Google Hacking



ffranz

[Follow](#)

Sep 29, 2018 · 2 min read

Google Dorks are a search strings that uses Advanced Search Operators to find beyond on Google database. Mmm... What an **Advanced Search Operator** is?!? Advanced Search Operators are operators to perform filters not only related to webpage text but other data indexed like **URL** or **WEB title**.

For example imagine you want to get all news on *cnn.com* that are talking about WannaCrypt, you can query Google using “**site**” operator to limit the search only in “*cnn.com*” domain.

| *site:cnn.com WannaCrypt*

With this query you obtain news that contains “WannaCrypt” word in their content and are located on “*cnn.com*” domain (including subdomains).

The image shows a Google search interface. The search bar contains the text "site:cnn.com WannaCrypt". Below the search bar, there are tabs for "All", "Images", "Maps", "Videos", "News", and "More". The "All" tab is selected. Below the tabs, it says "About 335 results (0.31 seconds)". The search results are listed below, each with a title, a URL, and a snippet of text.

Patch Now & Stop Ransomware - Free Tools to Stop WannaCrypt
[Ad go.ivanti.com/Security/WannaCrypt_tool](#) ▼
90-day License The best-in-industry patch management solution. Get started today
[Patch for Windows Server](#) · [Endpoint Security](#) · [Free 90-day Patch License](#)

WannaCrypt attack should make us wanna cry about our vulnerability ...
[www.cnn.com/.../wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-...](#) ▼
5 days ago - (CNN)On Friday, the world experienced the wrath of a well-coordinated ransomware attack, known as WannaCrypt. ... Before the malware could do damage in the United States, a lone British researcher, known as "MalwareTech," serendipitously identified its kill switch -- the registration ...

Massive ransomware attack hits 99 countries - May. 12, 2017
[money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/](#) ▼
7 days ago - ... that a large number of colleges and students in the country had been affected by the ransomware, which is also referred to as "WannaCrypt.

Ransomware: Attack hits 150 countries, Europol says world is in ...
[money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/](#) ▼
5 days ago - ... that a large number of colleges and students in the country had been affected by the ransomware, which is also referred to as WannaCrypt.

Global ransomware attack: 5 things to know - CNN.com
[www.cnn.com/2017/05/13/world/ransomware-attack-things-to-know/](#) ▼
6 days ago - The ransomware, called WannaCrypt or WannaCry, locks down all the files on an infected computer and asks the computer's administrator to ...

Global cyberattack: A super-simple explanation of what happened ...
[money.cnn.com/2017/05/14/technology/global-cyberattack-explanation/](#) ▼
5 days ago - Cyber bad guys have spread ransomware, known as WannaCry, to computers around the world. It locks down all the files on an infected ...

Now we know the potential of the Google Advanced Search Operators. So...
Let's see what we can do

WannaCry ransomware

Continuing with WannaCrypt we can perform queries to find potential victims. How can we do it? Easy, just trying to find servers that contains files encrypted by the Ransomware.

To do that we can use a couple of dorks:

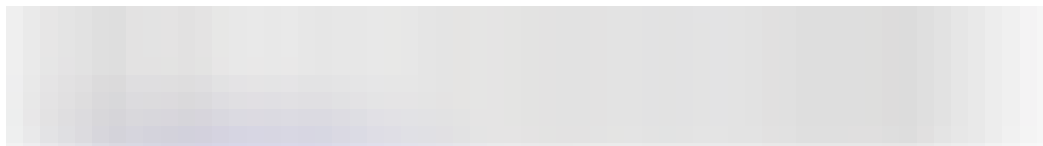
intitle:index of intext:@WanaDecryptor@.exe

intitle:index of intext:wncry

Google will return all servers that contains files with 'wncry' word in their names or where the binary file (@WanaDecryptor@.exe) associated with the malware was found.



Now you can navigate to results and see encrypted files and show files encrypted by Wannacry.

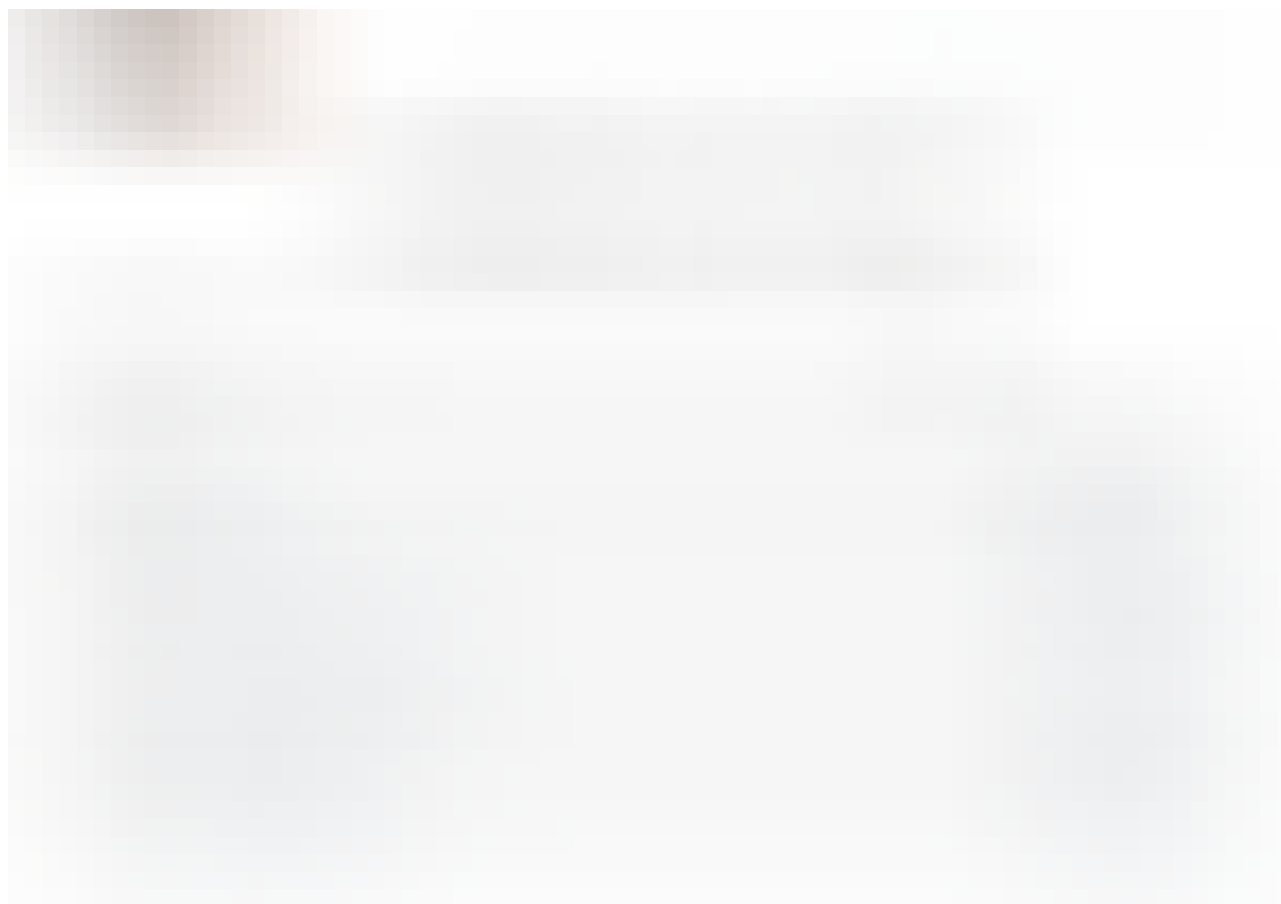




• • •

Google Hacking Database (GHDB)

GHDB is a database with thousand of Dorks categorized, explained and dated. This database is a great data source for the recognition phase in pen-testing for example. Here you can find the dorks used in this post and many more related confidential data, leaks, error files, etc...



Do you have more dorks related Ramsonware? Share with us!

Security

Wannacry

Cybersecurity

Google Hacking

Google Dork



ffranz

Cybersecurity stuff

Follow



ThreatsPerInch

Cybersecurity

Follow



Top on Medium



The Price We Pay for Multitasking at Work



David Staab

Apr 22 · 8 min read



3.6K



Top on Medium

You should never ever run directly against Node.js in production....

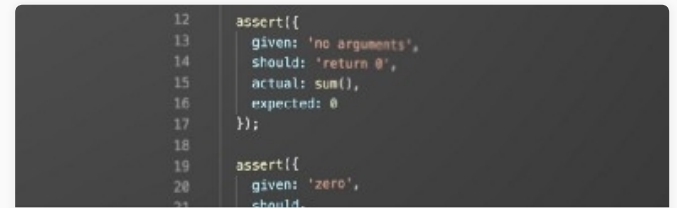


Burke Holland

Apr 22 · 10 min read



1.91K



Top on Medium

TDD Changed My Life



Eric Elliott

Apr 19 · 9 min read



9.1K



Responses

 Write a response...