WannaCry & Google Hacking

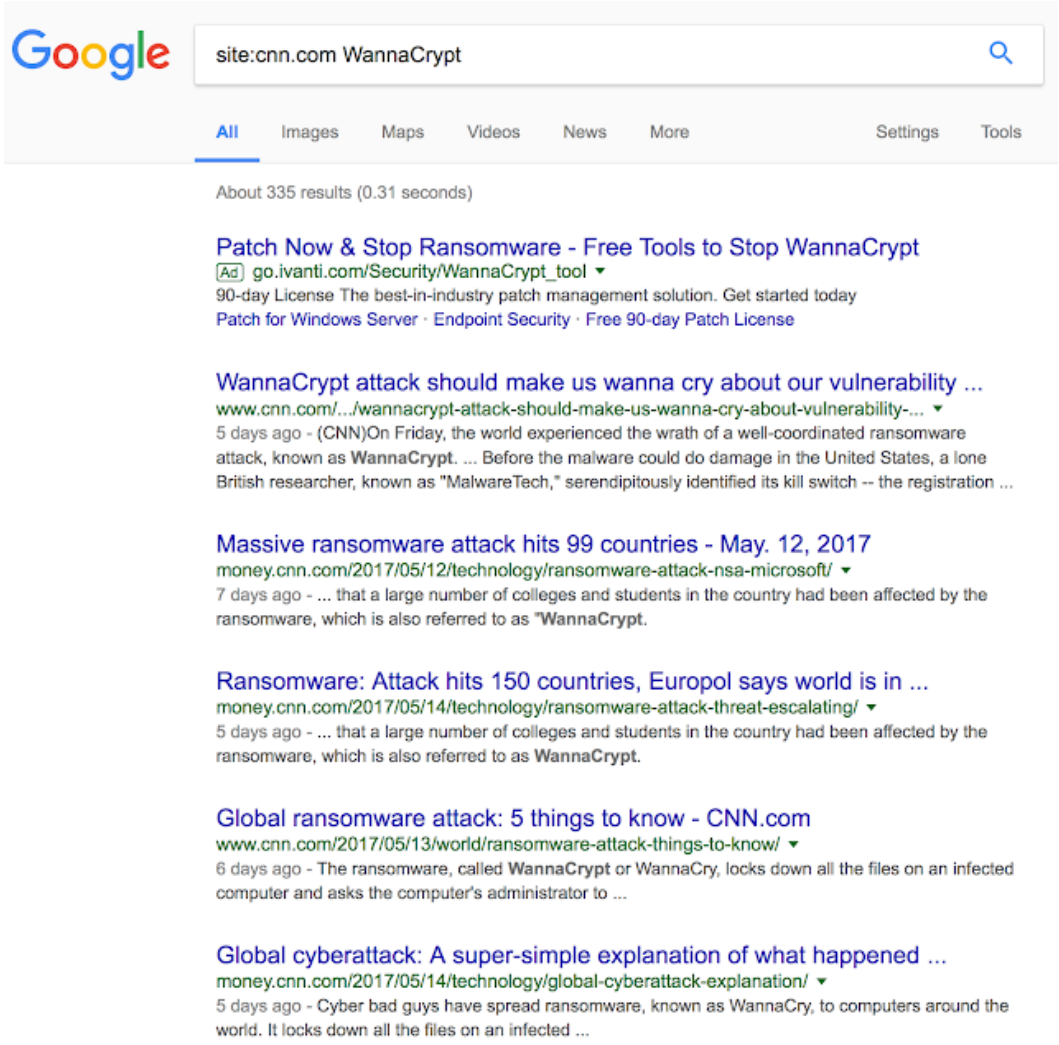
ffranz Follow
Sep 29, 2018 · 2 min read

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).



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

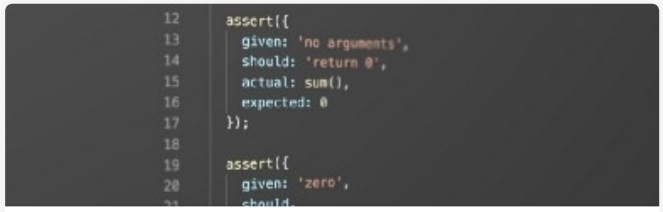
The Price We Pay for Multitasking at Work

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...