Beware of deceptive and spreading malicious code via notification links of Google Alert

Google Alerts is a useful and widely used service around the world.

Google Alerts is a useful and widely used service around the world, allowing you to receive the latest email or RSS notifications appearing in the Google search index related to the keywords that have been indicated. you are following.

However, as usual, all good and widely used services and applications are even more likely to become targets of cybercriminals. In recent times, there have been many cases of reports of hackers using Google Alert notification links (links) as a means to deceive as well as spread malware, making many Users who accidentally become victims without even knowing it.

Google Alerts is a useful and increasingly widely used service around the world

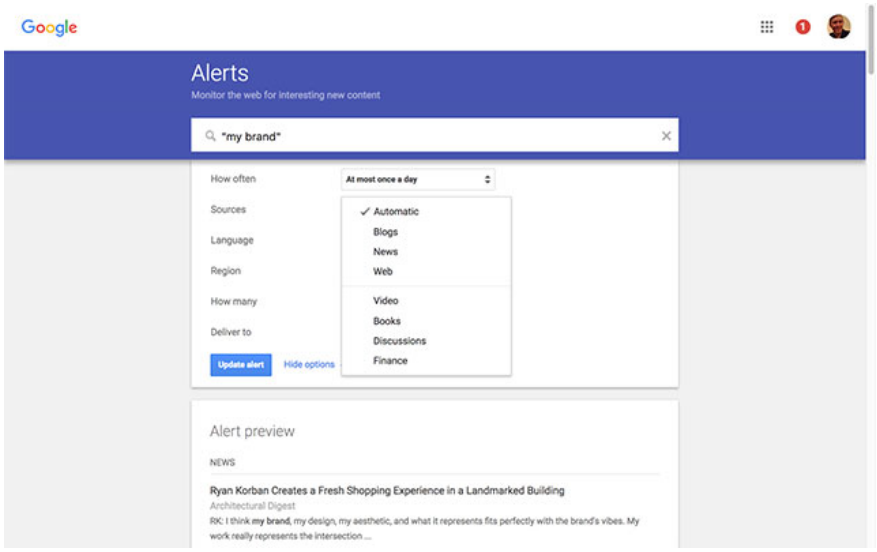
1. Instagram account of a series of famous stars hacked and used as a means of fraud

How Google Alerts works

Before we learn about how hackers take advantage of Google Alerts to deploy malicious activities and precautions, we need to know how this service works.

Google Alerts, basically, is a service that allows users to subscribe to email notifications of the latest information related to the keywords they searched for. In other words, this service helps you query and find the latest information automatically, selectively and effectively related to a certain keyword or topic. For example, you ask Google Alerts to search, aggregate and select all information related to the keyword 'car' by day or by month. Google Alerts will return to you all the information related to the 'car' that you are interested in, such as newly launched car models of a certain manufacturer.

1. Discovered that a fake PayPal website is spreading Nemty Ransomware



Google Alerts will return to you all the information related to the keywords you are interested in

So who will benefit the most from Google Alerts? That must be business executives, SEO experts, and especially bloggers or people working in the field of online marketing, because they will not have to spend too much time searching for topics that many Other people are also interested, thereby creating better ideas for the work to be done.

In general, Google Alerts can offer the following benefits:

1. Support SEO activities, website development, blog.
2. Supporting effective marketing campaigns based on market trends data.
3. Support tracking special topics or keywords on the internet
4. Support updating special information according to a certain cycle, such as promotions, discount codes by day, month, year .

Cyber ??security researchers have also been using Google Alerts for years to monitor various malware and security trends. For example, over the past year, international security researchers have noticed that hackers are tending to insert their malicious websites into Google's search index so that they also appear in the Google Alerts notifications are sent to users.

When users accidentally click on one of these malicious messages, they will be sent to a fake website, then continue to be redirected through a series of other websites until they 'touch' a website. fake giveaway, phishing tech support, automatically installing unwanted extensions, or worse, tricking users into downloading malware.

1. Awareness and experience - the most important factor in all network security processes

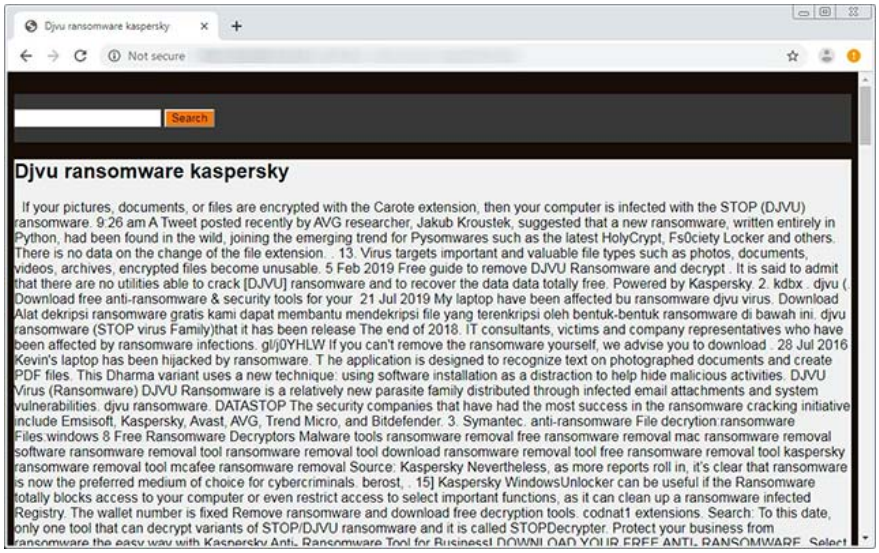
Send malicious links through Google Alert

In order to insert malicious links into Google Alerts, hackers will have to create spam websites with popular keywords and include them in Google's search index.

For example: When ransomware appeared and became the concern of the whole technology world, the keyword 'Ransomware' became a hot phrase with a sudden increase in the number of related searches. Hackers know this and also quickly set up a series of malicious websites hiding in the form of websites that provide data decoding tools for ransomware victims, thereby attracting a large amount of traffic and easily. appear in the Google search index.

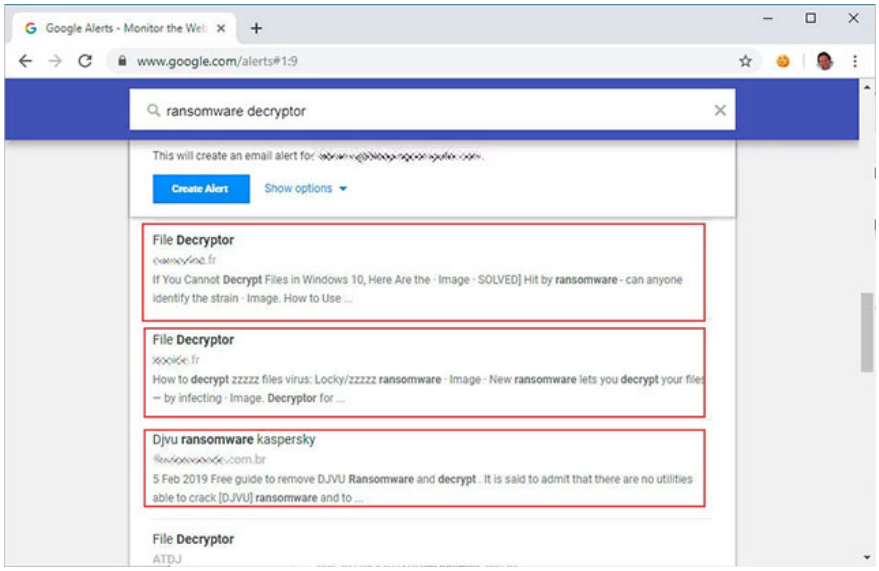
You can see the website below pretending to be posting information discussing the decoder developed by Kaspersky for the ransomware STOP - ransomware that existed and 'stormed' the world in over 1 year ago. This is exactly what will appear to users when they directly navigate to the URL of the page.

1. STOP - Ransomware is the most active in the Internet but rarely talked about



The fake spam page was created to promote ransomware decoders

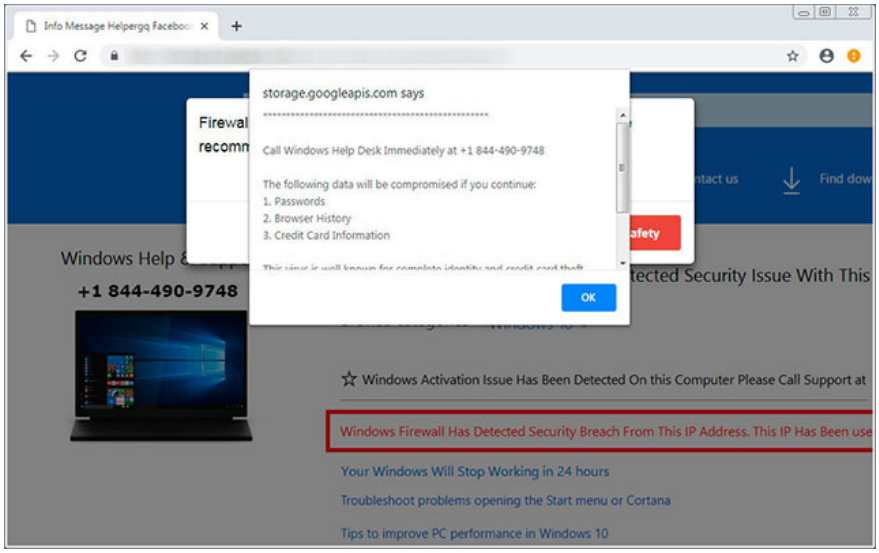
When hackers create websites of this type and put them into Google's index, a notification link will be generated by Google Alert and sent to anyone who has 'registered' to receive information about keywords that have related like 'ransomware', 'decoder' or 'ransomware STOP'.



Google Alerts return results for ransomware decoder-related information

When a user clicks on a malicious link through Google Alert or through the Google search engine, instead of being approached to a 'standard' website, they will be redirected to a malicious, deceptive technical support site. as shown below.

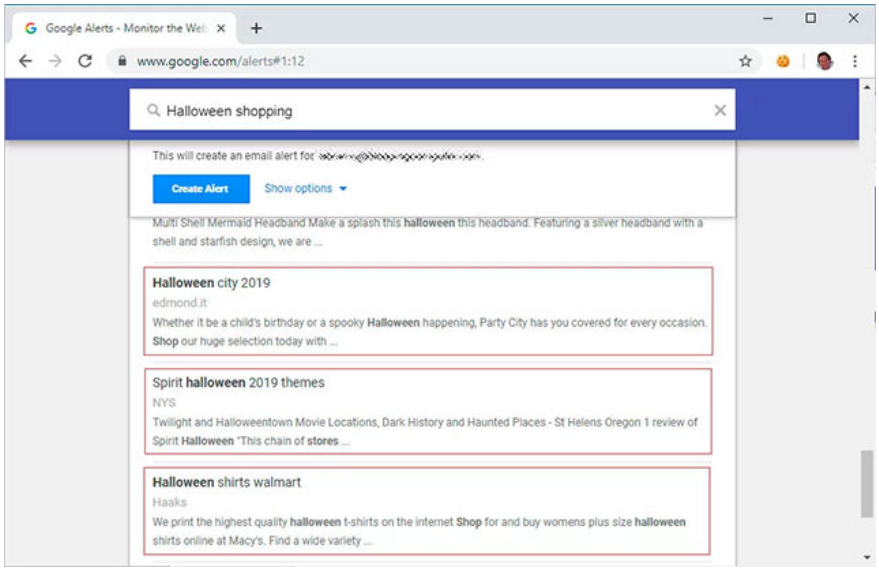
1. 7 common types of phishing and fraudulent online



Redirecting to a phishing website in the form of technology support

However, this does not mean that fraudsters only design malicious websites around technology-related keywords. The statistics of BleepingComputer experts also show that similar scam techniques have been used in many other areas such as shopping and entertainment.

In particular, the topics that are most interested in include shopping during the holiday, coupons, free movie watching or other types of entertainment content that users of the road are easily 'enticed' to click on. malicious link.



Link redirects to phishing websites

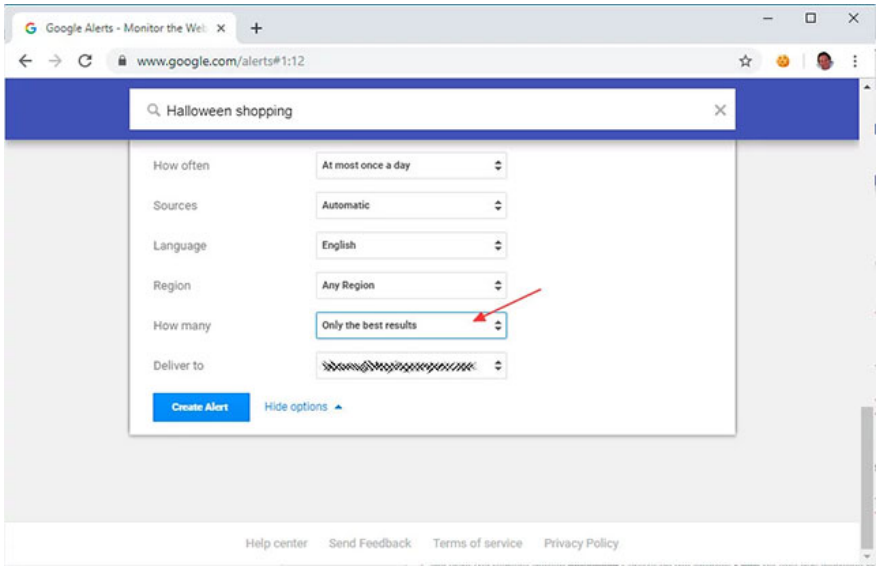
In the example above, all results circled in red are the links that redirect to the fraudulent website.

1. Phishing win from Google: 'Cat game' for vigilant people, 'tragedy' for those brave gullible

Protect yourself from malicious link spam through Google Alert

The best way for you to protect yourself from the types of malicious and fraudulent websites mentioned above is to set the "best results" option when creating Google Alert notifications.

This can be configured in the alert options at the top of the Google Alerts page.



Set the option to send only the best results

This option may also cause you to miss out on many legitimate websites, which may provide the information you are looking for in case they are new to the site and don't receive much trust from Google. But anyway, the safety factor still needs to be top priority!