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

The fight against STOP ransomware in particular and other ransomware strains in general is still very difficult and no appointment of an end date.

Have you ever heard of a ransomware called STOP? Perhaps not yet because very few people write about this ransomware, most researchers 'evade' it in reports, and especially STOP mostly targets victims through the crack software, adware packages and shady websites.

1. No More Ransom - the flagship of the battle against ransomware

The fight against ransomware is still very tough

The reason ransomware strains such as Ryuk, GandCrab or Sodinkibi have received great attention from cybersecurity organizations because they often require huge ransom payments, can be millions of dollars. , making individuals, businesses and even organizations and government agencies suffer. In addition, when it

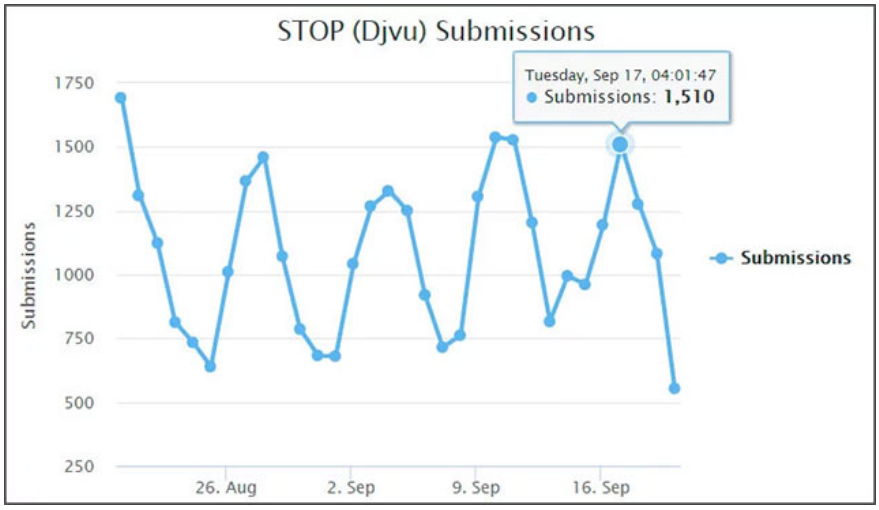
comes to ransomware, people often pay much attention to the ransomware factor, so the dense coverage of the ransomware mentioned above will also help newspapers and technology news pages to attract a large audience. than.

However, few people know that during 2018 and the first half of 2019, STOP is the most actively distributed ransom encryption software in the internet environment, this result is based on a comprehensive report on the requirements The support request sent to ID Ransomware was analyzed and analyzed by security expert Michael Gillespie at BleepingComputer.

In recent years, STOP ransomware has constantly 'evolved' and become a popular malicious code with a diverse number of variants.

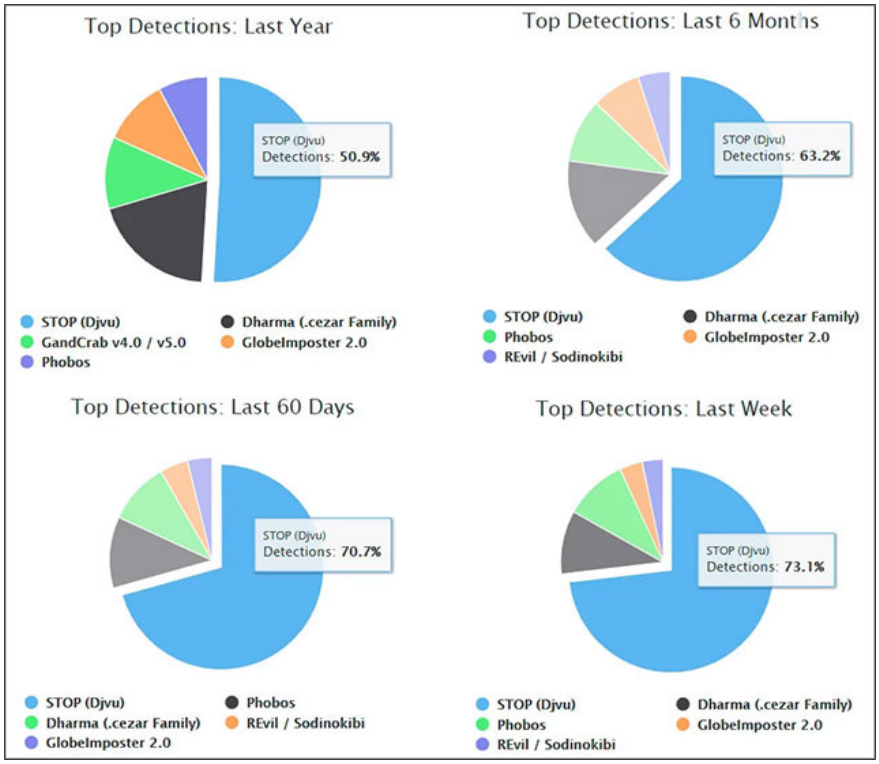
If you still do not believe this is the case, let's take a look at some of the statistics recorded on STOP ransomware. As noted by the ransomware ID ransomware identification service, there are nearly 2500 reports of ransomware being sent to this service center every day, including 60-70% of cases involving ransomware STOP, most are new victims and are seeking help.

1. GandCrab decoder officially released, ending a bad nightmare called GandCrab Ransomware



Number of STOP-related cases reported in September

This number completely overwhelms all statistics about other ransomware, regardless of popularity or huge ransom.



The number of reported STOP ransomware infections is steadily increasing

More attention is being paid to the number of reported ransomware STOP infections which is steadily increasing, completely outperforming other popular ransomware strains, as you can see in the statistics chart above. on.

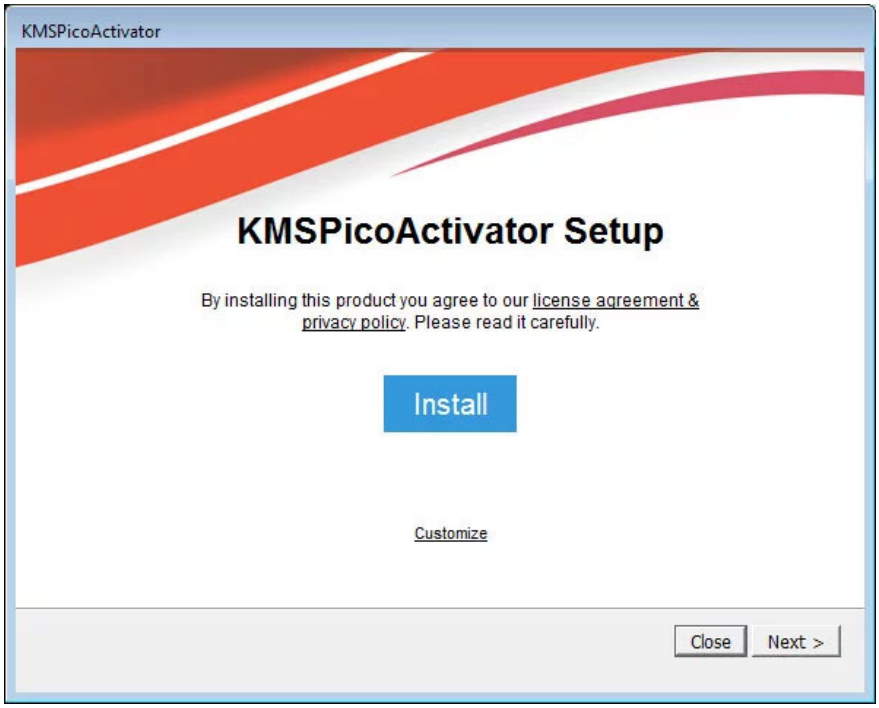
Application cracks, adware packages and shady websites - STOP's great spreading tools

As mentioned, STOP's distribution method is a bit different from many other ransomware. The people behind the ransomware have chosen to 'cooperate' with websites and adware package providers of unknown origin.

These sites are supposed to promote fake software or free programs, but in reality these are adware packages that can install malware and infect unwanted malware into the system. user's computer system. One of the malicious code installed through these packages is STOP Ransomware itself.

In addition, a number of application cracks are also an effective source of spread of this extortion malware, the most common of which is the crack version of KMSPico, Cubase, Photoshop and a few other common antivirus tools.

1. [Infographic] 7 effective ways to protect businesses from Ransomware



Application cracks are also a good source of STOP ransomware

However, not only cracked versions, many shady websites also offer free software download services, and in fact, these are adware packages that can install ransomware on the system of victims. multiply.

Not stopping there, some of these variants silently installed a password-stealing Trojan named Azorult on the victim's computer to steal information about accounts, e-wallets, computer files. desktop . Trojan Azorult is a malicious code that when spread to a victim's computer, it will attempt to steal the username and password information stored in the browser, as well as files on the system. victim's system . then upload the collected data to a remote server under the attacker's control.

It can be said that the factor that makes STOP dangerous and the most active ransomware lies in its flexible spread and its number of variants. Up to now, more than 159 STOP variants have been recorded, and this number is still increasing.

On the other hand, there's not much to say about how STOP works. It still encrypts the victim's file system just like any other ransomware, then appends a specific extension and provides a ransom note.

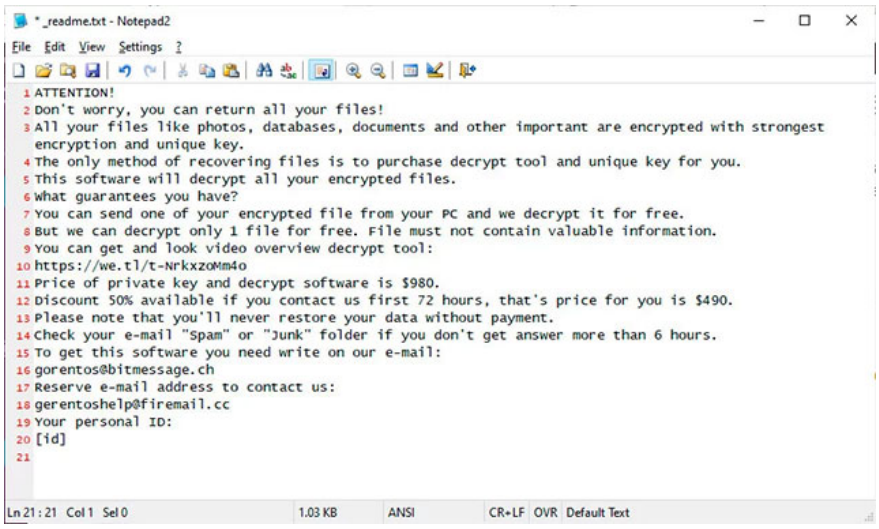
1. Even DSLR cameras can easily be attacked by ransomware

The journey to 'rescue' data is becoming more arduous than ever

Security researcher Gillespie has been successful in helping STOP victims recover encrypted files without paying a ransom through its STOPDecryptor decryption tool. This tool includes offline decryption keys that STOP itself uses when unable to communicate with malicious C2 servers.

However, this is not a simple task, with this ransomware sometimes released with 3-4 variants every day, and there are thousands of victims who need help at the same time.

1. LooCipher ransomware decoder officially launched, helping you get your data completely free



Ransomware STOP ransom notes

Unfortunately, the encryption has changed and in the near future Gillespie will no longer be able to provide as much support to STOP victims as it did before. This can certainly make many victims of this malware hopeless, especially in case they can not afford to pay the ransom 490 USD, and will double after 72 hours to 980 USD to regain data. has been encrypted. STOP victims are in need of help more than ever.

Many people may think that STOP victims deserve it because they have committed fraud in the first place, using crack software. But paying ransom data to hackers has never been a welcome idea, which only motivates attackers to create more ransomware.

1. Ransomware is showing signs of booming around the world, and paying is no longer the most viable option.

STOP victims are in need of help more than ever

The fight against STOP ransomware in particular and other ransomware strains in general is still very difficult and no appointment of an end date.

You finished reading the article "**STOP - Ransomware is the most active in the Internet but rarely talked about**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
