Shade ransomware, the nightmare of 5 years ago is showing signs of returning

Shade ransomware - extortion code recorded by Kaspersky Labs disappeared from the Internet five years ago, 2014, showing signs of returning again.

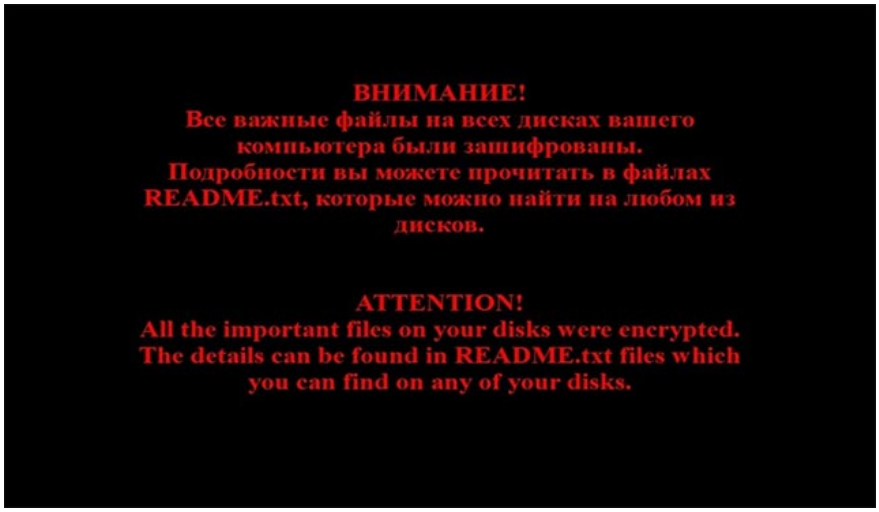
By 2019 half had passed, and so far, it can be seen that the frequency of large-scale ransomware infection has shown signs of significant decline in both quantity and damage compared to previous years, especially especially in 2017, when malware variants (especially Wannacry) caused trouble for millions of individuals, organizations, and businesses worldwide.

Of course it is still hard not to pay attention to the news about a public company or public agency becoming the latest victim of daily ransomware, and their struggle against ransom requests (money that the victims have to pay to recover their data) still seem to be the story of not ending. But with only the 'X company has become the target of ransomware', it's hard to say that this year's ransom attack trend is positive or negative. In fact, companies becoming victims of ransomware still appear every day, the most important thing of the year is that they are small or large-scale attacks.

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

As of now, 2019 has yet to record a massive ransomware campaign, even receiving good news when malicious code last year caused Gandcrab to announce a shutdown on the 1st. / 6 last. However, some of the older ransomware, which appeared before WannaCry for many years, may return to stronger in the second half of this year, 2019.

This scenario is gradually becoming a reality with the powerful re-release of Shade ransomware - the extortion code recorded by Kaspersky Labs disappeared from the Internet in the last five years, 2014. Right now, the security team Unit42 of Palo Alto has discovered a number of 'revival' cases of Shade ransomware in the United States, India, Thailand, Canada and Japan.



The hacker warning

1. New ransomware detection not only encrypts files but also helps 'clean up' the system

'Recent reports on malspam show that Shade ransomware has shown signs of returning to the internet environment and focusing on distribution via Russian emails. However, this dynamic code decoding guide always includes bilingual English and Russian text. The ransomware implementation software (EXE) has achieved significant consistency. All EXE templates that we have analyzed since 2016 use the same Tor address at cryptsen7f043rr6.onion as decryptor pages. At the same time, the desktop wallpaper of victim systems appearing during the infection process is the same since Shade was first reported as Troldesh in late 2014, 'said Brad Duncan, intelligence analyst. Network security belonging to Unit42 team, explained.

Shade ransomware's spread in this 2019 variant is fundamentally no different from any other contemporary malware that has been recorded. The Shade ransomware model is collected and shared by Unit42 team, which is 'multiplying' using a new, less-than-spam email method - but still relatively effective.

1. Microsoft warned about malicious spam campaigns using vulnerabilities in Office and Wordpad

The most powerful campaign to distribute this ransomware so far is recorded in February 2019 when security researchers have discovered a large number of spam emails sent from many different servers. . These spam emails contain pdf files or attached archives, in which the body of the email describes the attachment as a payment request from the service provider that the victim is using.

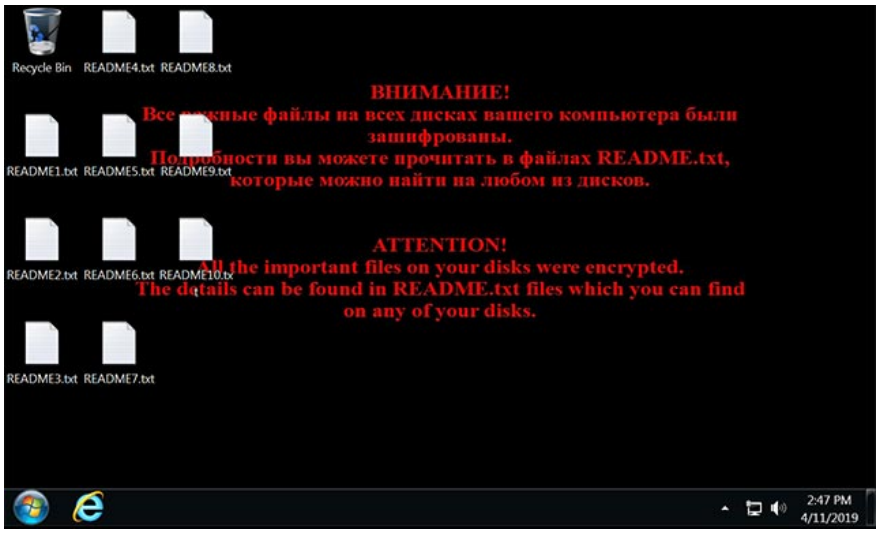
These pdf or zip files are of course not ordinary files. However, they only act as a launcher to execute malicious Javascript code - used to download the real malware from Shade ransomware from command and control servers (C2 server).

Shade ransomware's payload variant 2019 itself did not show any significant changes compared to the variant Kaspersky Labs first recorded in 2014. Specifically, when Shade's payload was successfully downloaded, It will

be executed automatically by the script in zip / pdf file as mentioned above - this is also the time when the file encryption process on the victim system and create the message text for the host thread takes place .

Next, the user-defined desktop wallpaper will be replaced with a black background with red text informing the system that it has been infected with Shade ransomware with the content: 'Attention! T?t c? t?p tin h?p l? trên ?? a c?a b?n ?ã ???c t?p tin. The details can be found in the README.txt files which you can find on any of your disks' (roughly translated! All important files on your system have been encrypted. Details of how to pay ransom can be found in the README.txt file that appears in all your hard drives'.

1. GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide



A computer has been infected with Shade ransomware

Unlike the previous version, the new Shade ransomware variant has a more direct destination, since most infections are in the United States. Previously, this malicious code also severely devastated Windows computer systems in India, Thailand and Japan. There are also clear signs that certain aspects of this particular, geographic location are targeted, in which victims are often businesses, groups and even People are operating in a number of industries such as telecommunications, wholesale / retail and education.

1. The cybersecurity tools that every business should know

Unit42's hypothesis has also shown that non-Russian-speaking countries are the most vulnerable subjects when receiving spam emails that carry Shade ransomware malware, suggesting it is likely that those behind the malicious code This is Russian or hosting a server in Russia.