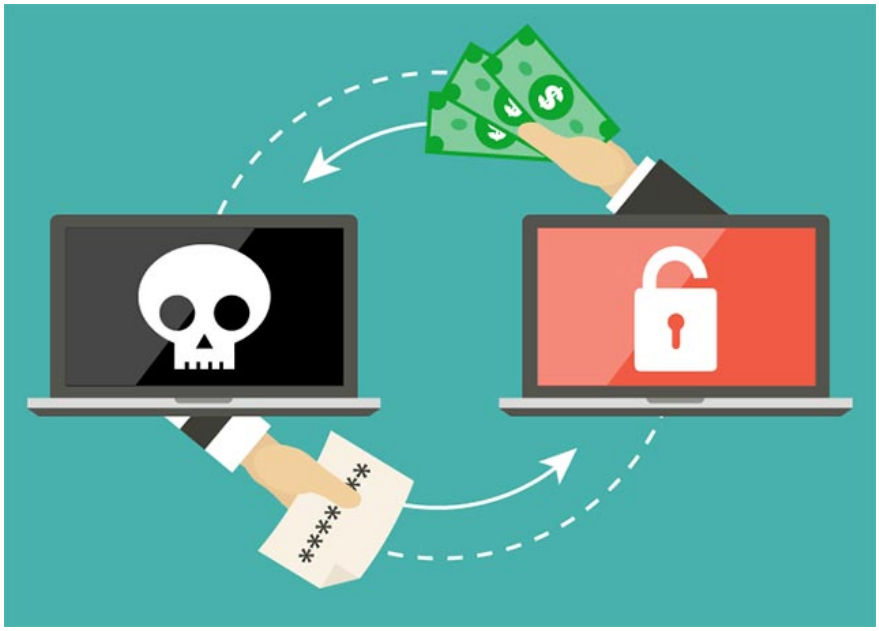
Ransomware (ransomware) is showing signs of explosion worldwide, paying is no longer the most effective option.

Malware file encryption has been, is and will continue to grow wildly.

A series of ransomware attacks have been reported in the past week, seriously affecting many US computer systems, including Georgia, New York, Tennessee and Florida. Along with that is the news of the global damage caused by ransomware, which is also increasing rapidly, making this form of ransom attack no longer simply a matter of security. security, but also become a threat, directly affecting many other areas of life.

File encryption malware has, is, and will continue to grow wildly in the near future. Recently, after Wannacry, GandCrab officially stopped working, other dangerous names almost immediately appeared and replaced, with even more sophisticated tricks, including Ryuk and Sodinokibi. Dharma / Phobos or even Shade . These malware not only target businesses like tradition, but also tend to cause more damage to individual systems.



Ransomware is a form of ransom data encryption attack

The agents behind the above threats have absolutely no distinction between the objectives. However, statistics from Coveware, a company famous in the area of ??ransomware incident response, show that victims from public areas (owned by the state) often pay data ransom. 10 times higher than private companies. Specifically,

the average for the second quarter of this year is 338,700 USD (in the US alone).

Check out some of the notable ransom attacks that took place recently in some US states to better understand the situation and the trend of this form of malicious attack.

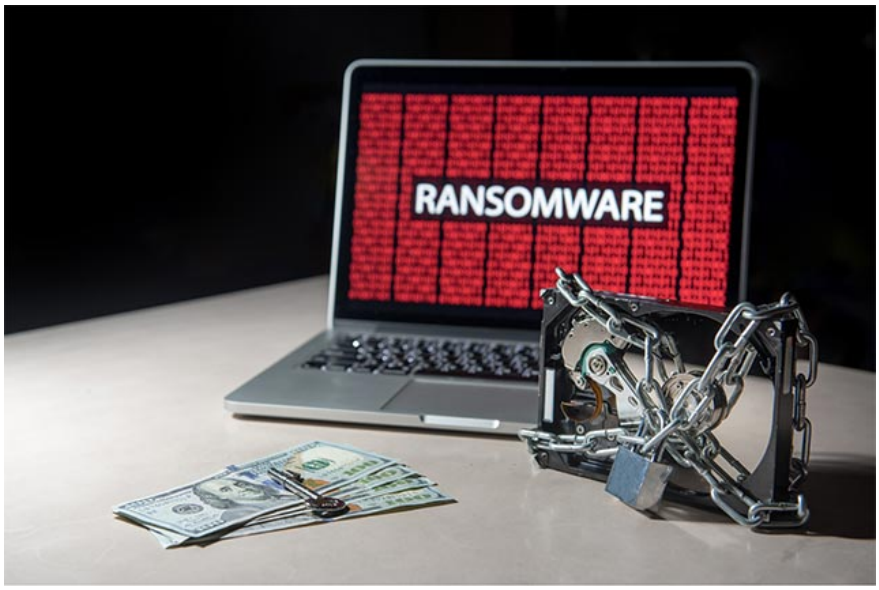
1. Shade ransomware, the nightmare of 5 years ago is showing signs of returning

Ransomware and coping options

1. Ryuk ransomware raged in Tennessee
2. Ransomware attacks radio centers in Florida
3. Ryuk ransomware attacked the New York library
4. Ransomware swept the state of Georgia
5. Paying the ransom is just a temporary solution

Ryuk ransomware raged in Tennessee

On July 18, officials Collierville, a town in Shelby, Tennessee, USA, confirmed that many computer systems of public agencies in the town were infected with a strain. Ransomware uncomfortable.



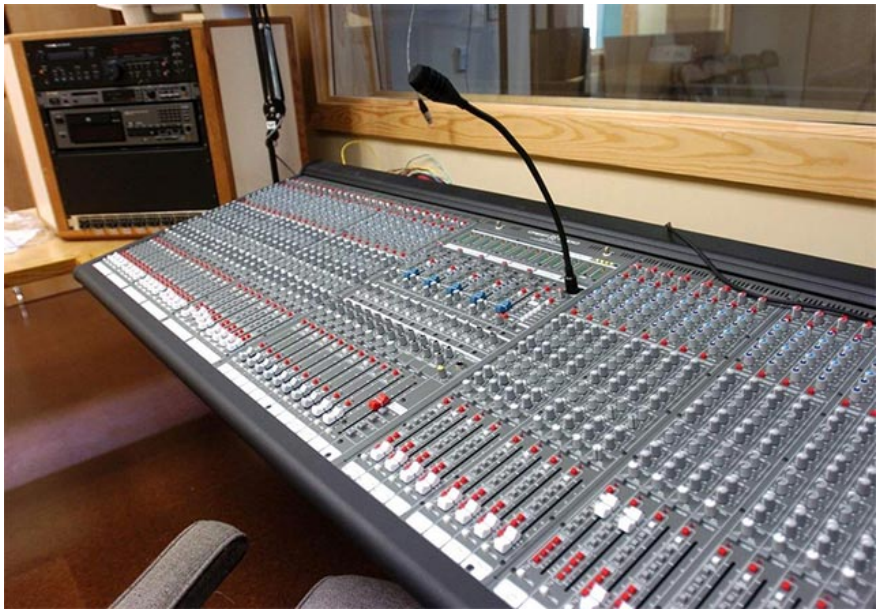
Collierville's IT management department has attempted to minimize the impact of malicious code, while also isolating some of the servers that were attacked. However, some services (licenses, public record requests and business services) have been seriously affected.

According to News Channel 3, the attack occurred in the morning and did not affect emergency services. The investigation was immediately conducted and according to reports, the ransomware strain behind this incident was Ryuk - a name that has been obsessed over the past few months.

1. Ryuk Ransomware added "selective" encryption capabilities.

Ransomware attacks radio centers in Florida

The computer system of WMNF 88.5-FM community radio station in Tampa, Florida, was enhanced at the highest level of security after an alarming ransomware attack occurred in the middle of last month.



The computer system of the WMNF community radio station is infected with ransomware

Specifically, the incident took place on June 18 last and did not seriously affect any sensitive data. However, the malware has access to an audio document storage system dedicated to advertising, news and work programs that have been recorded in advance.

Live broadcast broadcast systems have also been infected with malicious code, causing problems that seriously affect the broadcast schedule of the station, especially some planned or pre-programmed programs (WMNF 88.5 -FM will have to compensate). Economic damage is certain.

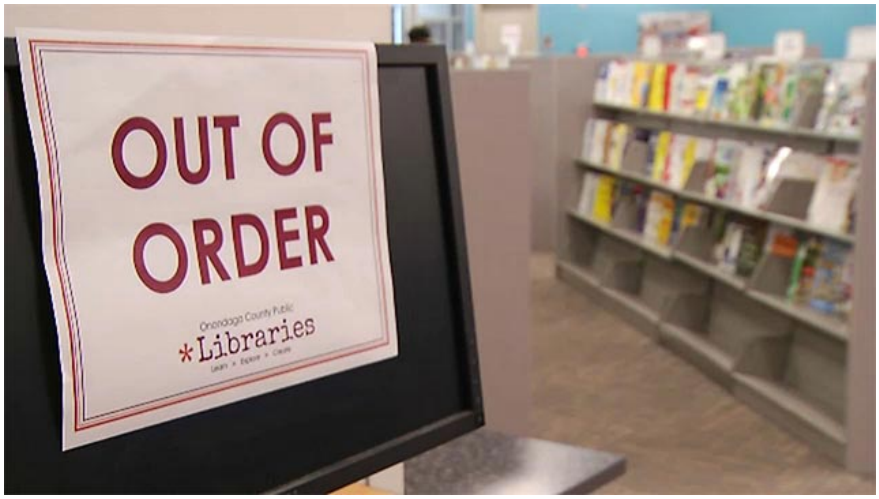
The Tampa Bay Times report said that although it does not own a backup for data that has been encrypted by malware, WMNF has decided not to pay the ransom. The reason given by Florida Law Enforcement Agency warned WMNF that the possibility of data loss could still occur even if they paid the ransom to the attackers.

In another remarkable news, the WMNF case was not the only case of ransomware in Florida in June. Before long, cyber criminals were thought to have pocketed at least $ 1 million (bitcoin) after successfully infecting malicious code into computer systems in Lake City (paid 42 cents). and at Riviera Beach (paid 65 bit of data ransom).

1. After WannaCry, Petya's "blackmail" malicious code is raging, this is a way to overcome and prevent it

Ryuk ransomware attacked the New York library

Another notable name joined Ryuk ransomware's victim list this year. Accordingly, this malicious code was found in nearly all computer systems of the Onondaga County (OCPL) libraries, New York, last Friday. Makes the operation of these libraries completely paralyzed.



The computer system of libraries in Onondaga County stopped working completely

The FBI quickly joined the incident, sending IT investigation teams to collect data and restore the majority of computer systems in these libraries.

As of yesterday, July 21, OCPL said their online system has started to return to normal operation. Library members can now access the OverDrive account and check items with a web browser.

OCPL did not disclose whether they paid the ransom to get back the data or the FBI did it. However, according to experts, it is likely that OCPL must accept to pay a large amount of money because the digital archives in these libraries are very valuable.

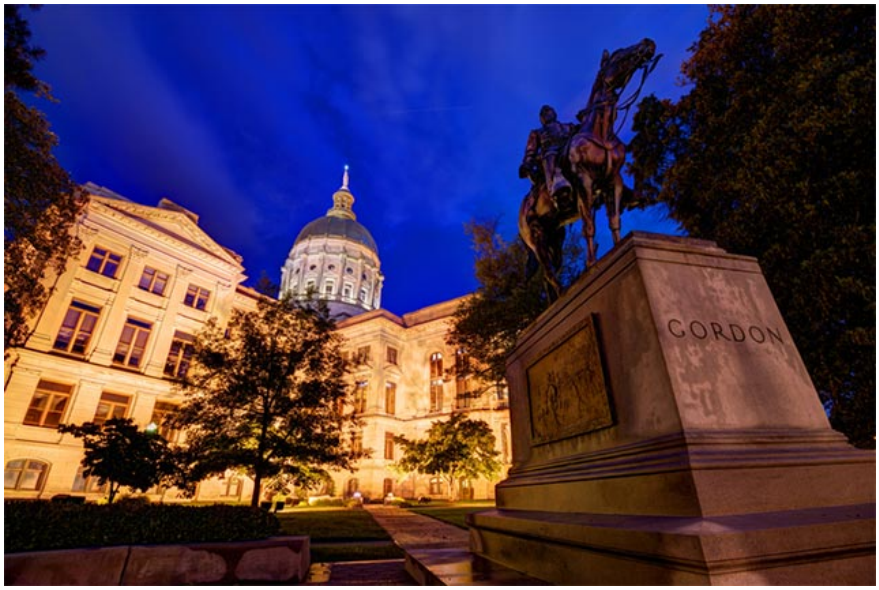
In a related move, Ryuk was also the ransomware strain responsible for the attack on the New York City School District of Onondaga County last week. Makes learning and teaching locally paralyzed.

1. Cr1ptT0r Ransomware spreads on D-Link NAS devices, targeting embedded systems

Ransomware swept the state of Georgia

Georgia is also one of the most vulnerable sub-groups from ransom data encryption attacks that are raging across the United States as well as in many other countries around the world since early 2019 to date. .

According to the latest information from Henry County, Georgia officials, the county's public computer system has been completely encrypted. The attack took place on Wednesday morning (around 3 or 4 am) and computer systems were still unable to function until yesterday afternoon, July 21.



The malicious code was crippled for the Henry County administrative network

More dangerous, the majority of encrypted computer systems are being used in a number of essential areas such as budget management, spending, management and administrative plans. Thus, the encrypted data is quite valuable and it is likely that local authorities will accept ransom payments in the future.

Melissa Robinson, public information officer of Henry County told local news agency that some of the county's departments and agencies would have to move to moderation, only working on normal paperwork if the current situation still exists. continue. This person did not clearly explain the nature of the case but stated that the FBI had actively contacted Henry County and they would take over the local computer system if necessary.

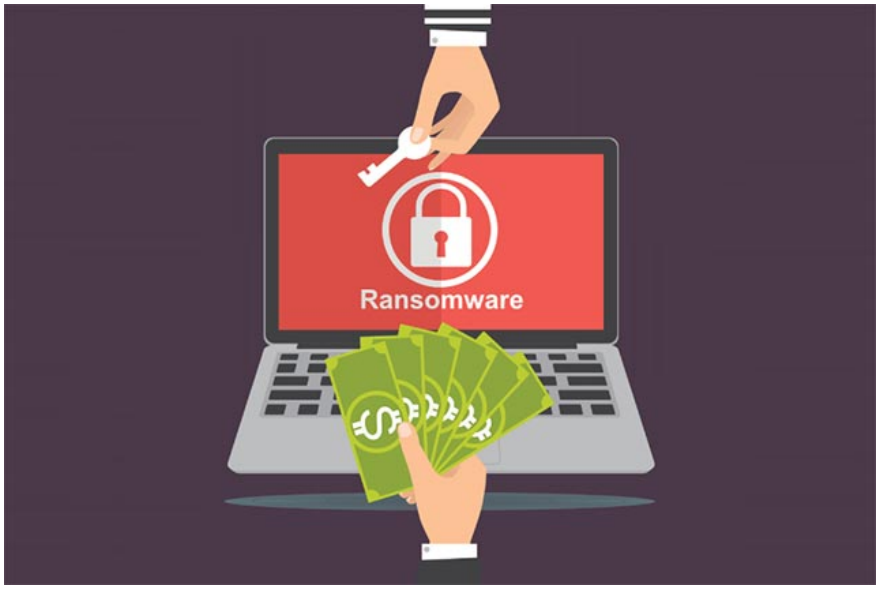
1. New ransomware detection not only encrypts files but also helps 'clean up' the system

Paying the ransom is just a temporary solution

Ransomware has been and will continue to be a serious threat to computer systems worldwide. However, this malicious code can also be easily suppressed and coped if the victim owns a backup plan in full for his or her data system, and it is important not to accept the ransom, Because as we know, the ultimate purpose of ransomware is to make the victim hook. Without paying the data ransom means that the source of the malicious code is cut off, the attacker will not be able to collect illegal profits.

More remarkably, paying for the key to decrypt the data is just a temporary solution in case the data is encrypted too important, or the paralyzed system causes too much damage, but cannot help solve the root problem in the long run. On the other hand, paying a ransom can also be seen as an act of encouraging the attackers to continue to push for profit through their illegal acts.

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



Paying data ransom is just a temporary solution, not of long-term value

Even after paying the data ransom, the general scenario that the victim will have to accept is financial loss and an investment in a better security system to protect themselves from other attacks in future.

Such is the case in Riviera Beach, Florida, USA. The ransomware attack on the city's computer system ended with local authorities accepting a huge amount of money, amounting to about $ 600,000 to get decrypted key words. They continue to invest nearly $ 1 million more in consolidating computer systems and upgrading new hardware pages to provide better security in the future.

In fact, most network attacks can be successfully deployed by exploiting reported but unresolved vulnerabilities, so installing the latest security updates will help Significantly reduce the possibility of attack. This is also the most effective and inexpensive defense measure.

In addition, it should be noted that there are projects and organizations specializing in extortion code like No More Ransom that can provide you with a free decryption key for many different versions of some ransomware strains. known.

Another project called ID Ransomware specializes in ransomware identification solutions for businesses by checking ransom notes or an encrypted file. For problems involving several popular ransomware strains such as Ryuk, Emisoft can support decoding files in 3% to 5% of recorded cases. Simultaneously, Ransomware ID can also help determine the effectiveness of decoding options according to each specific malicious code.

1. Overview of building enterprise security detection and response system

In terms of security as well as network security, organizations, businesses, and even individuals should make sure to keep an appropriate data backup plan, updated and changed regularly according to the activity. The reality of the system, and above all, it must be isolated from the main network.

Ransomware is a frightening form of cyber attack, but it's no big deal if you have a tightly built security system, as well as a logical data backup plan. Building such a system is not too difficult.

you for reading and for following us regularly.