Ransomware can encrypt cloud data

Ransomware is as small as a grain of sand, they are everywhere around us. And they can encrypt hard drive attacks but also attack other system drives, and cloud drives don't get out of sight.

Ransomware is as small as a grain of sand, they are everywhere. And they can be more coding than you think. The destruction of your personal files is a big loss, when Ransomware attacks your copies, this pain increases.

There are a number of variants of ransomware that not only attack hard drives but also attack other system drives, and cloud drives don't get out of sight. So this is the time for you to look at the exact file backups as well as where the copies are kept.

Ransomware attacks everywhere

We know a ransomware attack can be a havoc. Ransomware is a special obstacle because its target files are images, music, movies and document types. Your hard drive has not yet personal files, work and business as the main target for encryption. Once encrypted, you will see a ransom request for payment - usually in bitcoin difficult to track - to spread your files securely.

And even, there is no guarantee that you will receive an encryption password or decoding tool.

CryptoLocker

CryptoLocker is a variant of encrypted ransomware that can encrypt many of your hard drives. It first appeared in 2013, spread through infected email attachments. When CryptoLocker is installed on the computer, it can scan the hard drive for a specific list of file extensions. Furthermore, it scans all drives connected to the device, which may be USB or network.

A network drive with read / write access will be encrypted like a hard drive. It is a challenge for businesses where employees access shared network folders.

Fortunately, security researchers have released a copy of CryptoLocker's victim database and are compatible with each encryption. They create Decrypt CryptoLocker port to help victims decrypt their files.

Evolution: CryptoFortress

CryptoLocker appears and claims 500,000 victims. According to Keith Jarvis of Dell SecureWorks, CryptoLocker may have received $ 30 million in the first 100 days from extortion activity (it will raise $ 150 million if each victim pays $ 300 in ransom). However, removing CryptoLocker is not the beginning of

preventing ransomware from mapping network drivers.

CryptoFortress was discovered in 2015 by security researcher Kafein. It has the appearance and approach of TorrentLocker but one of the important advances; It can encrypt the network driver without mapping.

Typically, ransomware retrieves a list of mapped network drives such as C :, D :, E:, . Then it scans the drives, compares file extensions then code Customize the corresponding files. In addition, CryptoFortress lists all network shares that open Server Message Block (SMB) and encrypts whatever they find.

Locky

Locky is another variant of ransomware, famously changing each file to .locky, as well as wallet.dat - Bitcoin's wallet. The goal of Locky is also files on the computer or files on shared unmapped networks, changing files in the process. This chaos makes the recovery process more difficult.

Moreover, Locky has no decoder.

Ransomware on Cloud

Ransomware overcomes network physical and computer memory, and also passes cloud data. This is an important issue. The often-offered cloud storage is one of the safest backup options, keeping your data backed up, staying away from internal network sharing, creating a way to deal with dangers around. Unfortunately, the variants of ransomware have surpassed this security.

According to RightScale's State of the Cloud report, 82% of businesses are using multi-cloud strategy. And a further study (Slideshare ebook) by Intuit shows that by 2020, 78% of small businesses will use the cloud feature. This complete change of large and small businesses makes cloud services a major target for ransomware providers.

Ransom_Cerber.cad

Malware vendors will find a way to solve this problem. Social technology and phishing emails are the main tools and they can be used to avoid solid security controls. Trend Micro security researchers have found a special ransomware variant named RANSOM_CERBER.CAD. It is used to target home and business users of Microsoft 365, cloud computing and performance platform.

Cerber variant can encrypt 442 file types using AES-265 and RSA combinations, modify the Settings Zone of Internet Explorer on the computer, delete hidden copies, disable Windows Startup Repair and terminate Outlook programs , The bat!, Thunderbird, and Microsoft Word.

Furthermore, this is the behavior presented by other ransomware variants, Cerber queries the geographic location of the affected system. If the host system is a member of the Community of Independent States (former Soviet Union countries such as Russia, Moldova, and Belarus), ransomware will terminate itself.

Cloud as a poisoning tool

Ransomware Petya first appeared in 2016. A few things worth noting about this variation are first, Petya can encrypt the entire Master Boot Record (MBR) of the personal computer, causing the system to crash the screen. blue picture. This makes the whole system unusable. Then, when rebooted, Petya ransom records are displayed instead, with skulls and requests for payment with Bitcoin.

Second, Petya has spread to some systems via malicious infected files stored on Dropbox, pretending to be a summary. The link is disguised as the app's detailed information, while it actually links to a self-extracting executable file for ransomware installation.

Fortunately, an anonymous programmer found a way to crack Petya's encryption key. This way it is possible to detect the encryption key needed to unlock the MBR and free the captured files.

Using cloud services to spread ransomware is understandable. Users have been encouraged to use the cloud storage solution to back up data because it provides an additional layer of security. Safety is the key to the success of cloud services. Yet user confidence in the security of the cloud can be exploited for malicious use.

Summary

Cloud storage, network drivers are mapped or not mapped, and system files are still vulnerable to ransomware. This is no longer a new thing. However, malware distributors actively target backup files increase the level of anxiety for users. In contrast, additional precautions must be taken.

Home and business users should back up important files to a removable hard drive. Right now is the action to help you restore your system after an unwanted ransomware infection from an untrusted source.