BIZCOMMUNITY

Ransomware: more than just file encryption

By Doros Hadjizenonos

11 May 2017

In recent years, there has been a surge of ransomware attacks. It's been reported all over security blogs, tech websites and in the news.

Unfortunately, these attacks show no signs of slowing. If anything, they are getting worse. We estimate that the use of alternative ransomware, especially DDoS and IoT ransomware, will keep on growing in the near future, as IoT devices and web services continue to become more widespread.

© Dmitriy Shironosov via 123RF

One of the key factors driving the shift to ransomware is one of communications. Ransomware does not require an open line of communication after the infection. After the files are encrypted, it becomes the victim's responsibility to follow the directions in the ransom note to find the attacker in the TOR anonymised underground and complete the transaction.

There is no additional action required by the attacker, and the motivation to complete the payment is entirely on the victim if they wish to retrieve their files. These type of advantages and the resulting revenues have driven the popularity of ransomware.

Ransomware: more than just file encryption [part I]

Doros Hadjizenonos 6 Apr 2017

One of the reasons ransomware is getting past the defences of many organisations is that attackers have upgraded different aspects of ransomware to make it much more evasive. Traditional security products, such as antivirus and other signature-based protections, are fundamentally backwards-looking – they detect either previously seen malware or specific behaviours seen in previous attacks. Ransomware has found various methods to avoid detection and successfully infect computers. One of these methods is to embed ransomware inside slightly different versions of common documents, such as Word, Excel, PDF — but by changing the content it is packaged with the attachment no longer matches known hashes.

Modern ransomware is capable of reaching beyond an individual user's system, damaging large portions of an

organisation’s data through a single infection.

How to protect yourself

In the war against ransomware, there are a number of things you can do to prevent becoming a victim. Following these best practices can be a critical component in avoiding ransomware attacks and can help minimise the damage caused by a successful ransomware campaign against your organisation.

- **Backup your most important files:** If possible, enable automatic backups for your employees so you are not relying on users to remember to follow through with their backups. In the event of a ransomware attack, it may be possible to use these backups in lieu of paying the ransom, or at least allow you to decide for yourself whether the cost of restoring from backups is more or less than the requested ransom. Make an offline copy of your files on an external device and an online cloud stage service. (Note: external devices should be used for backup ONLY and be disconnected immediately after the backup is completed).

- **Employee education:** Employee education has been a key element in avoiding malware infections, and also applies to ransomware. The basics of considering where files came from, and whether or not they can trust the sender continue to be worthy of reminding users. In addition, ensuring that users only have access to the information and resources required to execute their jobs significantly reduces the possibility of lateral movement of a ransomware attack, and will minimise the potential impact of a successful attack on your organisation.

- **Exercise caution:** Don’t open emails you don’t expect to receive, and if you are asked to run macros on an Office file DON’T! The only situation in which you should run macros is in the rare case that you know exactly what those macros will do. Additionally, keep track of the latest major malware campaigns to ensure that you do not fall victim to a new unique phishing technique or download a malicious app.

- **Have a comprehensive, up-to-date, security solution:** High-quality security solutions and products protect you from a variety of malware types and attack vectors. Check Point Sandblast Zero-Day Protection efficiently detects and blocks ransomware samples, and extracts malicious content from files delivered by spam and phishing campaigns.

Response after infections

While preventing ransomware is the ideal scenario, knowing what to do in the event of a ransomware attack, and implementing tools capable of identifying an incident and containing ransomware infections can mean the difference between losing one computer and a more extensive infection.

If you are prepared for attacks through unprotected channels, detecting the ransomware within your network and blocking any communication between the ransomware and its command and control server using anti-bot technology will limit, and possibly block, its ability to operate.

Once you have managed to contain the ransomware, it is important to treat the whole infection and remediate the attack. Attacks must be dealt with as a whole, and protections must be implemented to keep it from reoccurring elsewhere.

Also read:

Ransomware: more than just file encryption [part I]

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...