GlobeImposter which has more than 20 variants, is still wildly growing

August 30, 2018

Aug 30, 2018Elley

Tweet

Learn more about 360 Total Security

Recently, 360 Security Team found the new variant of GlobeImposter ransomware family is actively spreading worldwide that has affected the great number of users. Moreover, the attack is expected to be more serious in the future.

GlobeImposter can be seen as one of the most powerful ransomware in these years. It uses a high-intensity algorithm for encryption. Once the files are encrypted, it is almost impossible to decrypt the documents. Then the hacker will send the payment method to the victim via email, and the victim is charged from 1 to 10 bitcoins.

Users should be aware of the severity of GlobeImposter ransomware attack due to not only its high-intensity data encryption algorithm but also its large number of variants. There have been more than 20 varieties of the family's variants since June.

The new variant discovered this time is with the extension NACRO. Although it is similar to the previous variants, the power of the attack is still not to be underestimated. If the computer is infected, the victim will find they cannot open their files, and the format will be tampered with seriously. After that, the attack will leave the contact form to the victim as usual.

Qihoo 360's Security Brain provides the latest techniques to protect our users
We found that GlobeImposter has various attack techniques, which is spread through cracking weak passwords.

Previously, a number of servers in a Chinese children's hospital were infected with the ransomware. The hospital's database files were encrypted, and its hospital information system could not be used normally. As a result, the patients of the hospital cannot pay medical expenses and make the appointment with doctors.

To keep away from the ransomware attacks, prevention is always better than cure. Qihoo 360's Security Brain is an all-in-one intelligent security system that comprehensively utilizes new technologies such as artificial intelligence, big data, cloud computing, IoT intelligent sensing, and blockchain to protect the country, national defense, critical infrastructure, society, and cities and personal network security. Among them, its situational awareness system can capture global malicious attacks or network anomalies in real time.

Reminder
We would like to recommend our users that they should install 360 Total Security to fight against the ransomware attacks. 360 Total Security would comprehensively protect our users from multiple dimensions such as the weak password automatic check, remote login protection, vulnerability intrusion prevention, and document protection.

Learn more about 360 Total Security