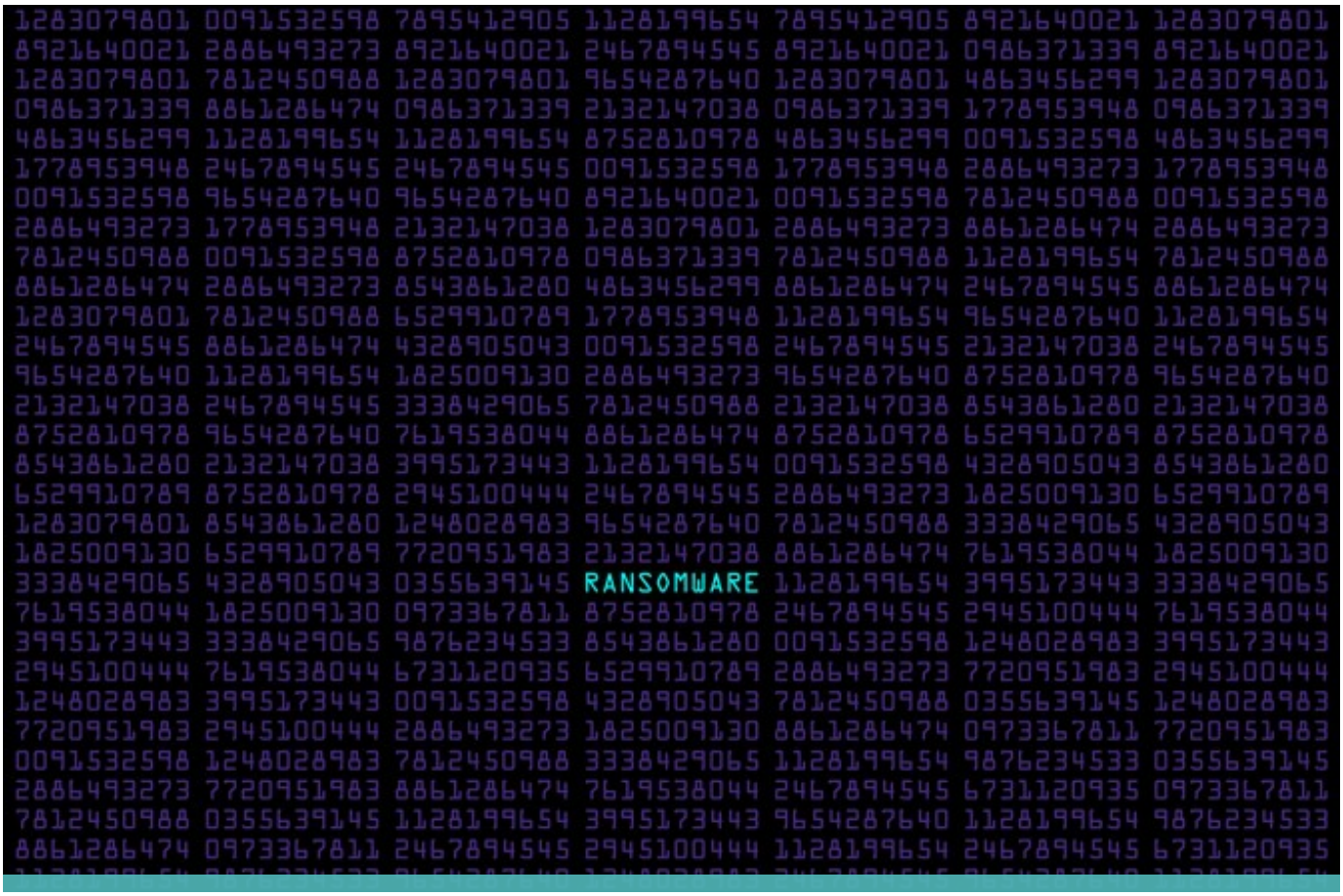
Ransomware roundup



Christine N. Czuprynski | Tuesday, July 18, 2017

We're just over halfway through 2017 and the cybersecurity story so far this year is ransomware, ransomware, ransomware.

What is ransomware?

Ransomware attacks occur when an unauthorized individual or group obtains access to a computer or network and all or some of the files stored there. The perpetrator encrypts files, making the data unavailable to those who need it, and demands the payment of a ransom in order to decrypt those files. The company or individual whose files are encrypted may be forced to pay the ransom unless there is some other way of restoring the locked files, such as through a recent file back-up that has not been compromised. Law enforcement generally advises against paying any ransom, since there is no guarantee that the files will be restored even when the ransom is paid, but the FBI has recommended paying under certain circumstances. Many infected companies without usable back-ups see no other option to paying the ransom.

The perpetrators of ransomware attacks often demand payment in bitcoin. The value of bitcoin fluctuates daily, but has continued to rise steadily over the last year. One bitcoin is valued at approximately $2,500 today. The represents an almost 300 percent increase from this time last year.

Ransomware infects systems through a variety of methods. Like any other type of malware, ransomware can exploit known software vulnerabilities, be launched when an unsuspecting individual clicks on a link in

a phishing email, and/or take advantage of lax security like the use of default passwords.

We've pulled together a few of this year's high-profile stories on ransomware.

WannaCry

The WannaCry ransomware attack hit in mid-May. The WannaCry variant exploited a software vulnerability. Instead of depending on users clicking on a phishing email link, WannaCry was a worm that traveled on its own to vulnerable computers. The malware infected the U.K.'s National Health Service, as well as many other public and private organizations, mostly in Europe, China and Russia. All told, over 150 organizations, some very large, were infected. Although early reports estimated the cost of WannaCry to exceed $4 billion, the actual bitcoin payouts made totaled less than $150,000. The low payout may be the result of affected entities having reliable and usable back-ups of data.

Petya: Not actual ransomware?

In June, another large-scale ransomware attack hit the presses. This one was Petya, and its impact was felt mostly in the Ukraine; reportedly 60 percent of infected computers were in that country. Though Petya looked like a classic ransomware attack, it soon became clear that files that had been infected by the malware could not be decrypted. The purpose behind Petya was likely not to make money, but to inflict damage on the computers and systems it infected.

Nayana's Big Payout

In what is thought to be the largest ransomware payout ever made public, in June the South Korean web hosting company Nayana paid $1 million to have its files unencrypted and released back into its possession after the ransomware variant Erebus infected its systems.

The perpetrators initially demanded 550 bitcoin, which was valued at about $1.62 million. Nayana negotiated down to around 400 bitcoin, or roughly $1 million.

What's Next?

There are no signs that ransomware attacks will slow down anytime soon. For large and small businesses alike, that means that there is one more reason to invest in strong cybersecurity. In addition to taking steps to better secure computers and networks, businesses should also ensure that they have strong data back-ups that will remain safe even if the network is infected.

Christine N. Czuprynski

Team member bio