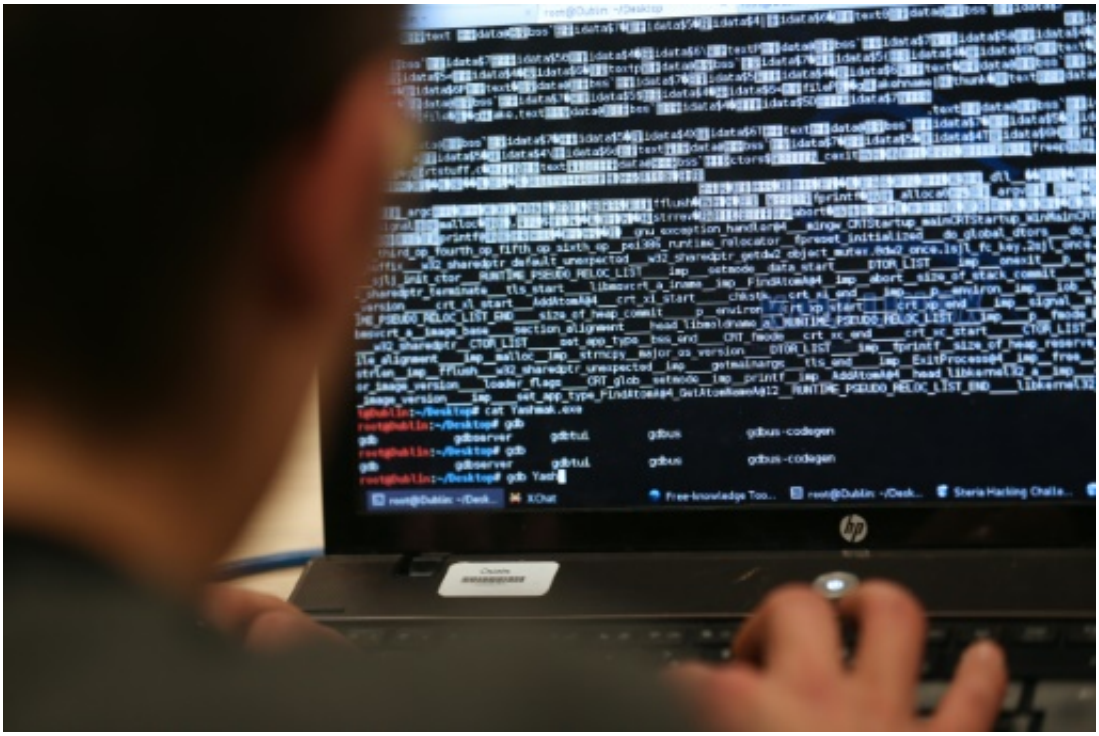
Epidemic of 'ransomware' is growing hacking threat

March 22 2016



The use of ransomware has become popular due to the hackers being difficult to find and ransomware software being available for free to obtain

Hackers are stepping up efforts to turn their exploits into cold cash, locking a user's data unless a ransom is paid, a report found Tuesday.

In the fourth quarter of 2015, so-called ransomware increased 26 percent quarter-over-quarter, according to Intel Security.

One single ransomware campaign last year netted $325 million, according to researchers.

The report did not estimate the overall value of ransomware, but the report found some six million attempts to install such malware, which encrypts the contents of a computer and locks the data down unless the user pays a ransom to obtain a decryption key.

Steve Grobman, chief technical officer at Intel Security, said the practice is growing due to several factors—easy access to the software, criminal networks which offer the service, and the difficulty of tracking down culprits who can hide in anonymous networks.

"In many ways this is a more lucrative business model than traditional forms of cybercrime," Grobman told AFP.

"And now we are seeing this move beyond consumers to 'soft targets' like hospitals and schools and police departments."

Grobman said these targets are chosen "because they typically don't have sophisticated cyber defenses that you would see at banks or defense contractors," but still hold data that can be held for hostage.

Although ransomware has been used for several years, the techniques have been refined and evolved to make them more usable.

Tracking down hackers has become difficult if they demand bitcoins, which have no traces in the banking system.

Ransomware software has become openly available as an "open source" took that any hacker can use for free.

And criminals with less technical sophistication can hire hackers who

make themselves available for the exploit—a business model known in the trade as "ransomware-as-a-service," the report said.

"Ransomware campaigns are financially lucrative with little chance of arrest, so they have become quite popular," Intel noted in the report.

Last month, Hollywood Presbyterian Medical Center acknowledged that it had paid $17,000 to hackers using ransomware, saying it was "in the best interest of restoring normal operations."

Grobman said the best defense against ransomware is preventive—backing up data in separate locations so that it can be restored, and using defensive software to filter out hacker emails.

But for someone infected with data locked by encryption, it is often a difficult choice.

"The bigger issue is that by paying the ransom, you are encouraging the cybercriminals, and it will drive the next generation of ransomware," he said.