Cyber Threats

Explaining how simple tactics led to unprecedented outcomes, a new report from global cyber-security firm Symantec said on Wednesday that cyber criminals are executing politically devastating attacks to undermine a new class of targets.

According to Symantec's "Internet Security Threat Report," cyber criminals revealed new levels of ambition in 2016 - a year marked by extraordinary attacks including multi-million dollar virtual bank heists and overt attempts to disrupt the US electoral process by state-sponsored groups.

"New sophistication and innovation are the nature of the threat landscape, but this year Symantec has identified seismic shifts in motivation and focus," Tarun Kaura, Director, Solution Product Management for Asia Pacific and Japan at Symantec, said in a statement.

"The world saw specific nation states double down on political manipulation and straight sabotage. Meanwhile, cyber criminals caused unprecedented levels of disruption by focusing their exploits on relatively simple IT tools and cloud services," Kaura added.

The report said subversion and sabotage attacks emerged at the forefront.

Cyber-attacks against the US Democratic Party and the subsequent leak of stolen information reflect a trend toward criminals employing highly-publicised, overt campaigns designed to destabilise and disrupt targeted organisations and countries.

Today, the largest heists are carried out virtually, with billions of dollars stolen by cyber criminals.

While some of these attacks are the work of organised criminal gangs, for the first time, nation states appear to be involved as well.

"This was an incredibly audacious hack as well as the first time we observed strong indications of nation state involvement in financial cyber crime. While their sights were set even higher, the attackers stole at least $94 million," Kaura added.

The report also found that one in 131 emails contained a malicious link or attachment -- highest rate in five years.

Source:

NDTV