Over 70% of Washington DC's CCTV Were Hacked Before Trump Inauguration

Posted by Hermes 02/19/2017

Just days before the inauguration of President Donald Trump, cyber criminals infected 70 percent of storage devices that record data from feds surveillance cameras in Washington D.C. in a cyber attack.

Any guess, What kind of virus could have hit the storage devices?

Once again, the culprit is Ransomware, which has become a noxious game of Hackers to get paid effortlessly.

Ransomware is an infamous piece of malware that has been known for locking up computer files and then demanding a ransom in Bitcoins in order to help victims unlock their files.

But over time, the threat has changed its way from computers and smartphones to Internet-of-Thing (IoT) devices.

Ransomware Infected 70% Surveillance Cameras in Washington D.C.

This time the hackers managed to plant ransomware in 123 of its 187 network video recorders, each controlling up to four CCTVs used in public spaces throughout Washington D.C, which eventually left them out from recording anything between 12 and 15 January.

Officials told the Washington Post that the incident forced them to take the storage devices offline, remove the infection and rebooted the systems across the city, but did not fulfill any ransom demands by the hackers.

While the storage devices were successfully put back to rights and the CCTV cameras were back to work, it is still unclear if any valuable data was lost or if the ransomware infection merely crippled the affected computer network devices.

Washington's chief technology officer Archana Vemulapalli said the officials are now investigating the source of hacking, assuring that the incident was limited to the storage devices tied to closed-circuit TV system and did not affect other D.C. government networks.

Rise in Ransomware: Both in Numbers and Sophistication

Ransomware is the hackers sure-shot way to get paid effortlessly. The threat has been around for a few years, but nowadays it has become one of the most used types of hacking methods.

Recently, hundreds of guests of a luxurious hotel in Austria were locked out of their rooms when ransomware malware hit the hotel's IT system, and the hotel paid the attackers to get back the control of their systems.

We saw an enormous rise in Ransomware threats, both in numbers and sophistication. You would be surprised to know about KillDisk data wiping ransomware that encrypts files and asks for an unusually large ransom of around $218,000 in Bitcoins, but did not provide decryption keeps even after the payment has made.

Another weird ransomware variant was Popcorn Time that was designed to give victims options to either pay a ransom to hackers or infect two more people and have them pay the ransom to get a free decryption key.

Prevention is the Best Practice

The only safe way of dealing with ransomware is prevention. The best defense against Ransomware malware is to create awareness within the organizations, as well as to maintain back-ups that are rotated regularly.

Most viruses and infections are introduced by opening infected attachments or clicking on malicious links usually served in spam emails. So, don't click on links provided in emails and attachments from unknown sources.

Besides this, always ensure that your systems and devices are running the latest version of Antivirus software with updated malware definitions. -Courtesy of SynEVOL
