Are you ALREADY infected by Gameover Zeus Malware?

Posted by admin | On 11 June,2014 | In Genral

In early June 2014, the U.S. Department of Justice announced that an international inter-agency collaboration named Operation Tovar had succeeded in temporarily cutting communication between Gameover Zeus, its command and control servers.

According to the FBI, Gameover Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. It is predominately spread through spam e-mail or phishing messages. It is believed to have been spread through the use of Cutwail Botnet.

The infected computers become part of a global network of compromised computers known as a Botnet-a powerful online tool that cyber criminals can use for their own nefarious purposes. In the case of Gameover Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to Gameover Zeus are estimated to be more than $100 million.

Unlike earlier Zeus variants, Gameover has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin, which means that instructions to the infected computers can come from any of the infected computers, making a takedown of the Botnet more difficult.

Gameover Zeus has mostly been used for online banking fraud and distribution of the CryptoLocker Ransomware.

CryptoLocker when activated encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. A message is then displayed on the computer screen which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid voucher) is made by the stated deadline and also threatens to delete the private key if the deadline passes. In case the deadline is not met, the malware offers to decrypt data via an online service provided by the malware's operators, for a significantly higher price in Bitcoin.

Although CryptoLocker itself is readily removed, files remain encrypted which researchers have considered impossible to break.

Evgeniy Bogachev has been added to the FBI's Cyber's Most Wanted list and was identified in court documents as the leader of a gang of cyber criminals based in Russia and the Ukraine, responsible for the development and operation of both the Gameover Zeus and Cryptolocker schemes. As per FBI, the actions to take down Gameover Zeus were truly collaborative. "Gameover Zeus is the most sophisticated Botnet the FBI and our allies have ever attempted to disrupt." said FBI Executive Assistant Director Robert Anderson. He added that the efforts announced are a direct result of the effective relationships that FBI has with it partners in the private sector, international law enforcement and within the U.S. government. However, since the author of Gameover Zeus has not been apprehended, Operation Tovar will dent the Botnet but not mitigate it completely. Present action will set back the criminals by a week or two, after which they will again resume their operations.

Apprehending these criminals is an important aspect of a Botnet takedown as malware development is a highly proactive process wherein newer vulnerabilities, enhanced anti-virus bypassing techniques and encryption schema has to be incorporated. Also, competition in the sale of exploits is a huge factor which forces the malware authors to continuously upgrade their kit; otherwise some other exploit kit will win the race in garbing the highly lucrative market.

The same was observed during the take down of Black-Hole Exploit Kit (EK). After the arrest of its author, Black-Hole EK simply ceased to exist. Unless and until, disregarding all the geographical and political boundaries, law and enforcement agencies work towards the common goal of take-down and arrest, just pulling down the Botnet infrastructure would be a futile exercise.

It should also be noted that twice in the past, the Law Enforcement Agencies had tried to bring down Zeus Botnet with limited effect and every time there was a takedown, the gang sprang back into action as if nothing had happened.

Hopefully, in near future the criminals behind this dreaded malware will be apprehended and put behind bars.