Are you ALREADY infected by Gameover Zeus Malware?

0

Posted by Suman Pokhiyal on June 11, 2014

Eearly 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.

However, to ensure IT security eScan suggests few Online Banking tips as below that can prove helpful:

- **Use Reliable Security Software**:
  - Use reliable anti-virus software that protects the system from all kinds of Malware attacks.
  - Ensure that the anti-virus and anti-malware programmes in your computer are regularly updated.
  - Download and install updates and patches for your operating system, applications and browsers regularly.
  - Enable Firewall in the computer system to ensure that you are safe on local networks and the Internet.
  - Keep the computer's security settings to a higher level. Configure your computer's Anti-virus settings to perform automatic system updates.

- **Keep Check on Websites You Visit**:
  - Some websites automatically download Malware onto your computer. Beware of such questionable websites.
  - While logging onto your web-based email provider or your online banking account, use the SSL protocol.
  - Never provide your account details, unless you are certain that the web site is genuine.
  - While banking online, check for URLs that begin with https, followed by a colon (:), and two slashes (//).

- **Use a secured Internet connection**:
  - Ensure that your network security settings are in place while you are using wireless network for online banking.
  - Always use online banking services of the banks that have encryption technology and good privacy policy.
  - Also, pay attention to the warnings by your Internet browser about unsecured sites.

- **Keep an Eye on Emails You Receive**:
  - Always remember that banks/other service providers never send emails that will ask for your personal details especially the password associated with your account. So be cautious of such emails.
  - In case of email-attachments, beware of the content of the email and when in doubt use any of the online services to open up these documents. There are numerous online services which will allow you to view PDF, DOCs or XLS.
  - Be cautious of phishing/unsolicited e-mails that promise you a credit card over the telephone as they may intend to charge your existing credit card without sending you anything. They may promise you specific discounts/ items/services and when you send your credit card information, you may never hear from them.
  - Beware of sudden disruption in your e-mail service from bank. In such situations, check with your bank if they had any recent request for a 'change of e-mail id', which you never did.
  - Avoid accessing the bank accounts with the hyperlinks sent through e-mails. Rather access the bank web site directly by typing in the Web address directly in the address bar.

- **Activate Notifications**:
  - Enable mobile alerts and notify your bank immediately upon suspicion of a fraudulent purchases / transactions.

- **Practice Efficient Password Management**:
  - Make sure to change your account passwords at regular intervals.
  - The passwords should not be easily predictable. It should be at least 8 characters long and a combination of numbers and alphabets.
  - Use OTP (one time password) facility.

- **Keep Your Confidential Information Safe**:
  - Keep your bank account detail safe. Avoid writing them down as it may fall into the wrong hands.
  - Never provide your bank account/ credit card information unless you are shopping on a legitimate web site.
  - In case you receive any e-mail from bank to verify/ provide your banking information, be cautious, as banks will never send such e-mails. It may be sent by identity thieves to steal your confidential information.
  - Avoid providing your bank account details and other private information through e-mail.
  - Never fill application forms for credit cards/ new bank accounts/ services received in e-mail, as it may be a trick by identity thieves to steal your confidential information.
  - Keep an eye on your bank statements/ account balance regularly. In case of any fraudulent/ unusual charges, immediately report it to your bank.

- **Practice Safe Online Banking**:

- Avoid banking online from a shared computer in public such as Internet cafes, etc.
- When using shared computer, make sure to disable 'File and Printer Sharing' option in the computer, when connected to the Internet.
- Every time you login to your online banking account, check your last login and logout record.
- Once you are done with online banking, always 'logout' to exit from your account rather than just closing the browser. Always clear the cache and browsing history.
- Avoid downloading/installing programmes from unreliable sources or opening suspicious files or e-mails.
- Avoid using debit card for online transactions; rather opt for credit cards/virtual cards.

- When **using Smartphone for online banking**, make sure that your device has legitimate apps.
-