Zeus

A Real Threat for Online Banking

Mohammad Jabed Morshed Chowdhury

Malware like Zeus has rapidly outpaced all other banking security threats, and according to a recent survey by PhoneFactor is regarded as the greatest threat to online banking today. Because malware has evolved to defeat most security measures currently in place, financial institutions must likewise evolve their security practices to stay ahead of these threats. As malware has become more pervasive and more sophisticated, out-of-band authentication and transaction verification have taken on a new level of importance for financial institutions and regulators. Instead of trying to get rid the world of malware, institutions can simply circumvent malware by 'stepping out' of band to authenticate transactions. In recent time, Zeus has involved as one of the most critical threat to online banking.

Zeus is Trojan horse computer malware that runs on computers running under versions of the Microsoft Windows operating system. While it is capable of being used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. It is also used to install the CryptoLocker ransomware. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009 security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco.com.

How it works : For instance, you might receive an e-mail claiming to come from an online retailer, or a social networking site, or a financial institution - but it has really been forged by the criminals to dupe you into becoming their next victim. A typical attack would see an email claiming to be an invoice, or an order confirmation - perhaps claiming that your credit card has been charged a large amount. If you click on a link in the email you will be taken to a booby trapped website which will silently exploit your computer, infecting it with the malware.

The virus lays dormant until it spots an opportunity to steal personal details such as online banking information and passwords. It then transmits this information back to the criminal network that uses it to drain the victim's accounts. It has already infected a number of computers and those who have it are putting valuable data, including precious photographs, music and personal files, at risk. In the worst cases, victims could lose access to their bank accounts which could be systematically drained. In a further twist, if the user is not a 'viable' victim then the software locks the information on the computer and holds it to ransom. At the moment the software demands one Bitcoin, an untraceable form of online currency favored by criminals, which is around £300. The U.S. Government admitted that at least one police force has been forced to pay this ransom to release sensitive files. It is thought that the gang first check if a target's keyboard is in Russian and only strike if it is another language. Worldwide, it is believed Gameover Zeus is responsible for more than one million computer infections, resulting in financial losses in the hundreds of millions of dollars.

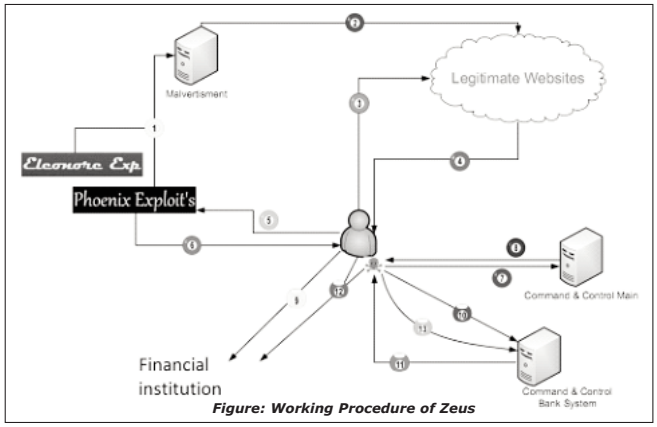

Figure: Working Procedure of Zeus

How can people protect their computers?

Many of those whose computers have already been infected will be contacted by their internet service providers. Computer users must install anti-virus software and update their operating systems to the latest versions to stop it regaining its hold. But this has to be done within two weeks, because there is only a limited period they can disable the attack for as hackers will be able to install new servers. Any good anti-virus program should be able to protect you from Gameover Zeus - provided you have kept it up to date.

The key thing is to ensure that your anti-virus is automatically updating itself, and you are applying the latest security patches from the likes of Microsoft and Adobe when they become available. The virus targets Windows. Mac users are not at risk from this particular threat. The NCA advised computer users to consult the Government-backed getsafeonline.org website. From that website, computer users can download tailored anti-virus software which has been provided for free by eight companies. Experts have also warned users to back-up all valuable data. To protect yourself you need to update your operating system and make this a regular occurrence, update your security software and use it and, think twice before clicking on links or attachments in unsolicited emails.

Who's the mastermind behind it?

Evgeniy Mikhailovich Bogachev is the man suspected of being behind a gang that has sparked a global cyber virus pandemic. But the FBI has already spent years looking for him who uses the online names 'lucky12345' and 'slavik'. The 30-year-old is wanted for his alleged involvement in a 'racketeering enterprise' that installed malicious software known as 'Zeus' on victims' computers. The FBI believes Bogachev knowingly acted in a role as an administrator while others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised websites.

Conclusion : Though Bangladeshi online banking sector has not been affected by notorious Zeus malware, but we should take precaution to protect ourselves for probable future attack. You should install a good anti-virus in your pc and install patches for operating systems to protect ourselves CJ