InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Security | Software | Storage | Hardware | Mobile | Unified Communications | I

Follow Us:

Newsletter Signup:

Security

A+ A-

Malware: A looming threat to online banking

There is a sudden increase in banking malware and web is no more a safe haven for online users especially when carrying out financial transactions, says Govind Rammurthy of eScan

By Govind Rammurthy , eScan, March 22, 2012

in - 1 Like 0 Tweet

We all know that the banking industry has grown leaps and bounds with the inception of electronic banking. From transferring of funds to making online purchases – all transactions are well taken care of without stepping out of one's comfort zone. However, there is one question we need to ask ourselves – do we ever consider updating our browsers or even patching the Windows Operating System to the latest fixes? Close to 85 percent of web users eliminate the fact of upgrading their applications and OS with the latest fixes, thereby increasing the possibility of being hacked almost three-fold.

Online banking snitchers are growing at a rapid pace and the sudden increase in banking malware is a proof enough of their existence. Take the instance of the fast spreading Citadel malware, the Trojan is built to target online users and has been evolving ever since its creators have trickled down code that was once implemented in Zeus – one of the oldest and most popular banking Trojan. Since its release, the Zeus source code has served as a base for the development of other banking Trojans, such as IceIx and the recent Citadel.

Just like Zeus, Citadel is sold as a crimeware toolkit in the underground market. The toolkit allows fraudsters to customize the Trojan according to their needs and command and control infrastructure. The malware authors of Citadel have gone a step further by creating an online platform through which customers or so called buyers can request additional features, report bugs and even contribute various modules to further enhance the functionality of the malware.

The malware features a number of improvements like the use of AES encryption for configuration files, blocking of anti-virus websites on infected computers, blocking of automated Botnet tracking services and the addition of remote screen video recording capability.

The Citadel malware comes in as a new breed in the evolution of malware. The Trojan is built to pop up as an online chat feature on banking sites. The malware uses a series of fake HTML and JavaScript injections, stalls online sessions and informs the user "security checks are being performed" – followed by the message – "The system couldn't identify your PC. You will be contacted by a representative to confirm your personality. Please pass the process of additional verification otherwise, your account will be locked. Sorry for any inconvenience, we are carrying about security of our clients." The only aspect that could raise an air of doubt is the use of poor language. Once successful, the malware presents itself as a live chat session luring the user to sign/verify fraudulent transactions.

It goes without saying that the web is no more a safe haven for online users especially when carrying out financial transactions. The overall threat financial malware are bringing is far greater than what Zeus brought along in 2010. Moreover, it is only a matter of time before malware authors implement Citadels code to create even more complex malware.

It is therefore crucial to keep your browser up to date and run strong anti-virus software on your computer. Be alert and do not click any unsolicited messages, especially the ones with grammatical errors and spelling mistakes.

Govind Rammurthy is MD & CEO eScan