Scottish Business Resilience Centre

Creating a secure Scotland for business to flourish in

Gameover ZeuS / Cryptolocker Advisory

As you may be aware from recent news reports, law enforcement agencies and computer security companies have recently taken action to disrupt two serious computer viruses.
These viruses, called “Gameover ZeuS” and “Cryptolocker”, are designed to steal money from online bank accounts or encrypt all of the files on a computer until a ransom is paid.
The action taken means that the viruses don’t work at the moment. However, the criminals who use them are expected to issue new versions soon, meaning there is a short window for internet users to take action now to protect their home computers.

How do the viruses work?

Both of these viruses are generally delivered by very convincing fake emails, either as an attachment disguised as a legitimate document or as a link in the email itself. These contain code which scans the computer and attempts to infect it with one of these viruses. If the computer is not up to date with the latest security patches, it will be infected and the user will be unaware.
Gameover ZeuS allows criminals full access to an infected user’s computer. Keystrokes can be captured, including online banking log in credentials and passwords. The virus can also trick users into entering banking security codes from a card reader into their computer which are then transmitted to the criminals and used for fraud.
Cryptolocker encrypts (or “locks”) all of the files on a user’s computer making it unusable. It is important to note that this includes any files stored on removable or networked drives that are connected to the computer at the time of the malware infection. A message informs the user that their files are encrypted and that they have a short time in which to pay a sum of money to receive the password to unlock them. So far, only the password is capable of unlocking files encrypted by this virus.
Both of these viruses can only affect computers running Microsoft operating systems*.

What can I do to protect myself?

There are several things you can do to protect your computer from infection by these viruses and to protect yourself if your computer is infected:

- **Don't open any attachments from emails you didn't reasonably expect. Some of the fake emails recently appear to have come from banks, HMRC and delivery companies, so don't click on a link or attachment unless you're 100% sure it's genuine.**

- **Install anti-virus software and set it to update automatically.**

- **If your bank offers security software, consider installing it as it is designed to protect you from the latest viruses and fake websites which criminals can use to steal your money.**

- **Keep your computer itself up to date – Microsoft offer automatic updates for their operating systems and software. Update your other software programs as well.**

- **Back up your files regularly, using a drive you can manually remove easily, or software which password protects your backup drives.**

- **Never store any passwords or sensitive information, like banking details in unencrypted files, such as Word documents.**

- **These types of computer frauds generally start via phishing emails**

More advice, and free tools to help you detect and remove these viruses can be found at http://www.getsafeonline.org/

*The following operating systems are susceptible to Gameover ZeuS:

- Microsoft Windows: 95, 98, Me, 2000, XP, Vista, 7, and 8
- Microsoft Server: 2003, Server 2008, Server 2008 R2, and Server 2012

Other operating systems, such as Apple Mac OSX and iOS (used on Macs, iPads and iPhones), Linux and Android cannot be infected with these specific computer viruses. Users of these systems are also advised to keep their systems up to date and use anti-virus software.