INTERNATIONAL ACTION AGAINST 'GAMEOVER ZEUS' BOTNET AND 'CRYPTOLOCKER' RANSOMWARE

02 Jun 2014

Press Release

The Hague, the Netherlands

On Friday, 30 May 2014, law enforcement agencies from across the world, supported by the European Cybercrime Centre (EC3) at Europol, joined forces in a coordinated action led by the FBI which ensured the disruption of the Gameover Zeus botnet and the seizure of computer servers crucial to the malicious software known as CryptoLocker.

US authorities identified a 30 year old suspect from Anapa, Russian Federation, as a leader of the cyber criminals behind Gameover Zeus. The FBI has added him to the Cyber's Most Wanted section on their website.

Gameover Zeus, also known as 'Peer-to-Peer Zeus', is an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. It then uses those credentials to initiate or re-direct wire transfers to accounts controlled by cyber criminals. It is the latest version of a malware family which appeared already in 2007 and security researchers estimate that between 500 000 and one million computers worldwide are infected. Known losses caused by the malware are estimated to be around EUR 75 million.

The Gameover Zeus network of infected computers also distributes the ransomware known as CryptoLocker. In October last year, EC3 sent out an alert concerning CryptoLocker which encrypts all files of the victim's computer, extorting an amount of USD 750 or more to receive the password necessary to unlock the files. Security researchers estimate that, as of April 2014, CryptoLocker had infected more than 234 000 computers. Furthermore, the FBI estimates that over USD 27 million in ransom payments were made in just the first two months since it emerged.

Besides US authorities, investigators from Canada, France, Italy, Japan, Luxembourg, Germany, New Zealand, the Netherlands, Ukraine and the United Kingdom participated in the operation. Crucial support was delivered by industry partners such as Dell SecureWorks, Microsoft Corporation, McAfee, Symantec and other companies* to prevent the malware re-installing itself after it had been removed from the victims' computers.

On the action day, EC3 activated its operational centre where representatives from the various countries worked shoulder to shoulder with Europol officials towards a successful outcome.

The Head of the European Cybercrime Centre (EC3), Troels Oerting, said: "This big, and very successful, operation has been an important test of the EU Member States' ability to act fast, decisively and coordinated against a dangerous criminal network that has been stealing money and information from victims in the EU and all over the globe. Over many days and nights cyber police from several EU countries in EC3 operation rooms maximized the impact of this joint investigation. We get better and better after each such operation, and many more will undoubtedly follow".

Also EU Home Affairs Commisssioner Cecilia Malmstroem expressed her satisfaction with the successful operation:

"No internet user should have to fear becoming a victim of extortion or banking fraud. This joint operation clearly demonstrates how important it is to cooperate across borders to tackle cybercrime - because no country is an island. By having the European Cybercrime Centre go after these criminals, we are making the internet more secure. But with the mounting threats ahead, is more important than ever to intensify this cooperation."

Read more in Cyber bits: Encryption ransomware - CryptoLocker and at FBI website.

*Abuse.ch, Afilias, Carnegie Mellon, Crowdstrike, Delloite, F-Secure, Georgia Tech, Heimdal Security, Level 3 Communications, Neustar, Shadowserver, Sophos, Trend Micro.

CRIME AREAS	Economic Crime • Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
GENERAL TERMS	Operation
ENTITIES	European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware