EUROPOL

INTERNATIONAL POLICE OPERATION TARGETS POLYMORPHIC BEEBONE BOTNET

09 Apr 2015

Press Release

On 8 April, Europol’s European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), joined forces with the Dutch authorities and the FBI, and U.S-based representatives at the National Cyber Investigative Joint Task Force- International Cyber Crime Coordination Cell (IC4) along with private sector partners, to target the Beebone (also known as AAEH) botnet, a polymorphic downloader bot that installs various forms of malware on victims’ computers. Initial figures show that over 12 000 computers have been infected, however it is likely there are many more.

In the operation, led by the Dutch National High Tech Crime Unit, the J-CAT’s Cyber Liaison Officers worked together with Europol officials and representatives from Intel Security, Kaspersky and Shadowserver. Eurojust also provided assistance to the operation. The botnet was 'sinkholed' by registering, suspending or seizing all domain names with which the malware could communicate and traffic was then redirected. Data will be distributed to the ISPs (Internet Service Providers) and CERTs (Computer Emergency Response Teams) around the world, in order to inform the victims. The botnet does not seem the most widespread, however the malware is a very sophisticated one, allowing multiple forms of malware to compromise the security of the victims’ computers.

Europol’s Deputy Director of Operations, Wil van Gemert, says: "This successful operation shows the importance of international law enforcement working together with private industry to fight the globa threat of cybercrime. We will continue our efforts to take down botnets and disrupt the core infrastructures used by cybercriminals to carry out a variety of crimes. Together with the EU Member States and partners around the globe, our aim is to protect people worldwide against these criminal activities."

To illustrate the sophisticated nature of this threat, there are currently over 5 million unique W32/Worm-AAEH samples, with more than 205 000 samples from 23 000 systems in 2013-2014. These systems are spread across more than 195 countries, demonstrating the threat’s global reach. The United States reported the greatest number of infections followed by Japan, India and Taiwan.

F-Secure, Intel Security, Symantec and TrendMicro have released a remedy to clean and restore infected computers' defences. For those who fear their computer may have been infected, EC3 recommends downloading specialist disinfection software. For further information please visit www.getsafeonline.org, www.cyberstreetwise.com or https://www.us-cert.gov/.

Do you want to know what a botnet is and how it is used by cyber criminals? Please check our infographic and our explanatory video!

For further information, please contact: Lisanne Kosters, Europol Corporate Communications, +31 70 302 5001

CRIME AREAS Cybercrime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
GENERAL TERMS Operation
ENTITIES European Cybercrime Center (EC3) • Joint Cybercrime Action Taskforce (J-CAT)

Source URL: https://www.europol.europa.eu/newsroom/news/international-police-operation-targets-polymorphic-beebone-botnet