NEW GENERATION OF MALWARE TARGETED BY INTERNATIONAL LAW ENFORCEMENT

14 Oct 2015

Press Release

Europol's European Cybercrime Centre (EC3) is actively supporting the National Crime Agency (NCA) and the Federal Bureau of Investigation (FBI) in their activities aimed at bringing down Dridex banking malware which has inflicted £20m of estimated losses in the UK alone.

Dridex, considered the successor of Cridex banking malware, has been developed by technically skilled cyber criminals in Eastern Europe to harvest online banking details, which are then exploited to steal money from individuals and businesses worldwide. Global financial institutions and a variety of different payment systems have been particularly targeted by this malware.

Computers become infected with Dridex malware when users receive and open documents in seemingly legitimate emails. This malware most frequently infects users running Windows operations systems.

While the use of 'old-school' banking Trojans such as Zeus, Citadel or Spyeye are in decline due to withdrawn support – either voluntarily or as a result of law enforcement action, a new generation of malware has come to the fore. Dridex is one of them, and is becoming more prominent in law enforcement investigations given the sensitivity of the harvested data, increasing degree of sophistication and growing number of cases.

With the support of EC3 and the Joint Cybercrime Action Taskforce, alongside a number of international law enforcement agencies and key private partners, the NCA is conducting activity to 'sinkhole' the malware, stopping infected computers – known as a botnet – from communicating with the cybercriminals controlling them. This activity is in conjunction with a US sinkhole, currently being undertaken by the FBI.

This activity is part of a sustained and on-going campaign targeting multiple versions of Dridex and the cybercriminals behind it, who operate in hard to reach parts of the world.

Members of the public are reminded they should be vigilant and not open documents in emails, or click on links, if they are unexpected or if they are unclear about its origin.

For those who fear that their computer may have been infected, EC3 recommends downloading specialist disinfection software. For more information, please

visit www.getsafeonline.org or www.cyberstreetwise.com.

For more information regarding malware and other types of cyber threats, please consult the latest edition of Europol's Internet Organised Crime Threat Assessment.

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

Source URL: https://www.europol.europa.eu/newsroom/news/new-generation-of-malware-targeted-international-law-enforcement