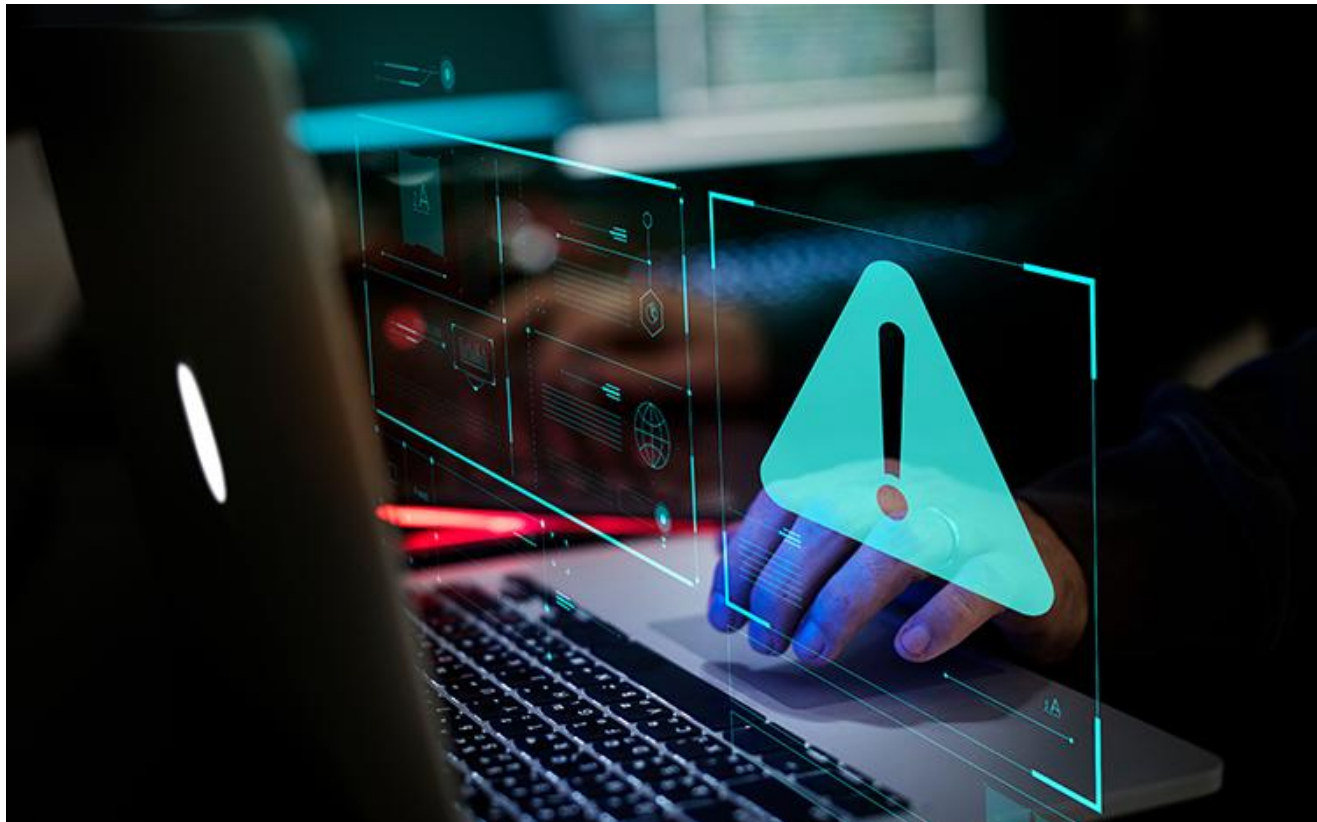


World's most dangerous malware EMOTET disrupted through global action

 eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action



27 January 2021 | PRESS RELEASE

Joint Eurojust Europol Press Release



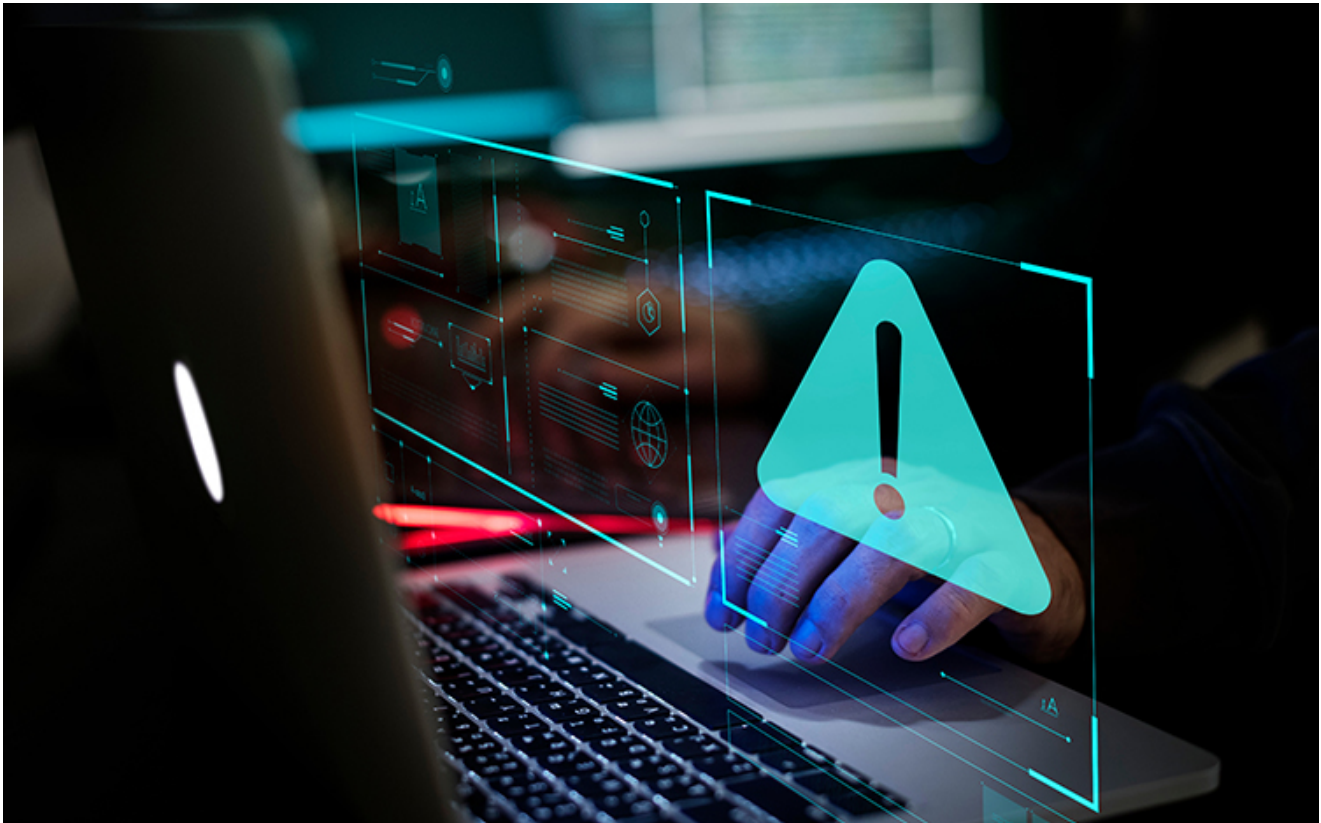
Law enforcement and judicial authorities worldwide have this week disrupted one of the most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried

out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

EMOTET has been one of the professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top level criminal groups to deploy further illicit activities such as data theft and extortion through ransomware.

Spread via Word documents



The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments. A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns have also been presented as invoices, shipping notices and information about COVID-19.

All these emails contained malicious Word documents, either attached to the email itself or downloadable by clicking on a link within the email. Once a user opened one of these documents, they could be prompted to "enable macros" so that the malicious code hidden in the Word file could run and install EMOTET malware on a victim's computer.

Attacks for hire

EMOTET was much more than just a malware. What made EMOTET so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer.

This type of attack is called a 'loader' operation, and EMOTET is said to be one of the biggest players in the cybercrime world as other malware operators like TrickBot and Ryuk have benefited from it.

Its unique way of infecting networks by spreading the threat laterally after gaining access to just a few devices in the network made it one of the most resilient malware in the wild.

Disruption of EMOTET's infrastructure

The infrastructure that was used by EMOTET involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups, and to ultimately make the network more resilient against takedown attempts.

To severely disrupt the EMOTET infrastructure, law enforcement teamed up together to create an effective operational strategy. It resulted in this week's action where by law enforcement and judicial authorities gained control of the infrastructure and took it down from the inside. The infected machines of victims have been redirected towards this law enforcement-controlled infrastructure. This is a unique and new approach to effectively disrupt the activities of the facilitators of cybercrime.

How to protect oneself against loaders

Many botnets like EMOTET are polymorphic in nature. This means that the malware changes its code each time it is called up. Since many antivirus programmes scan the computer for known malware codes, a code change may cause difficulties for its detection, allowing the infection to go initially undetected.

A combination of both updated cybersecurity tools (antivirus and operating systems) and cybersecurity awareness is essential to avoid falling victim to sophisticated botnets like EMOTET. Users should carefully check their email and avoid opening messages and especially attachments from unknown senders. If a message seems too good to be true, it likely is and emails that implore a sense of urgency should be avoided at all costs.

As part of the criminal investigation conducted by the Dutch National Police into EMOTET, a database containing e-mail addresses, usernames and passwords stolen by EMOTET was discovered. You can check if your e-mail address has been compromised at www.politie.nl/emocheck [unfortunately this link no longer points to an existing page at the external website]. As part of the global remediation strategy, in order to initiate the notification of those affected and the cleaning up of the systems, information was distributed worldwide via the network of so-called Computer Emergency Response Teams (CERTs).

The following authorities took part in this operation:

- Netherlands: National Police (Politie), National Public Prosecution Office (*Landelijk Parket*)
- Germany: Federal Criminal Police (*Bundeskriminalamt*), General Public Prosecutor's Office Frankfurt/Main (*Generalstaatsanwaltschaft*)
- France: National Police (*Police Nationale*), Judicial Court of Paris (*Tribunal Judiciaire de Paris*)
- Lithuania: Lithuanian Criminal Police Bureau (*Lietuvos kriminalinės policijos biuras*), Prosecutor's General's Office of Lithuania
- Canada: Royal Canadian Mounted Police
- United States: Federal Bureau of Investigation, U.S. Department of Justice, US Attorney's Office for the Middle District of North Carolina
- United Kingdom: National Crime Agency, Crown Prosecution Service
- Ukraine: National Police of Ukraine (*Національна поліція України*), Prosecutor General's Office (*Офіс Генерального прокурора*)

© EUROJUST 2022