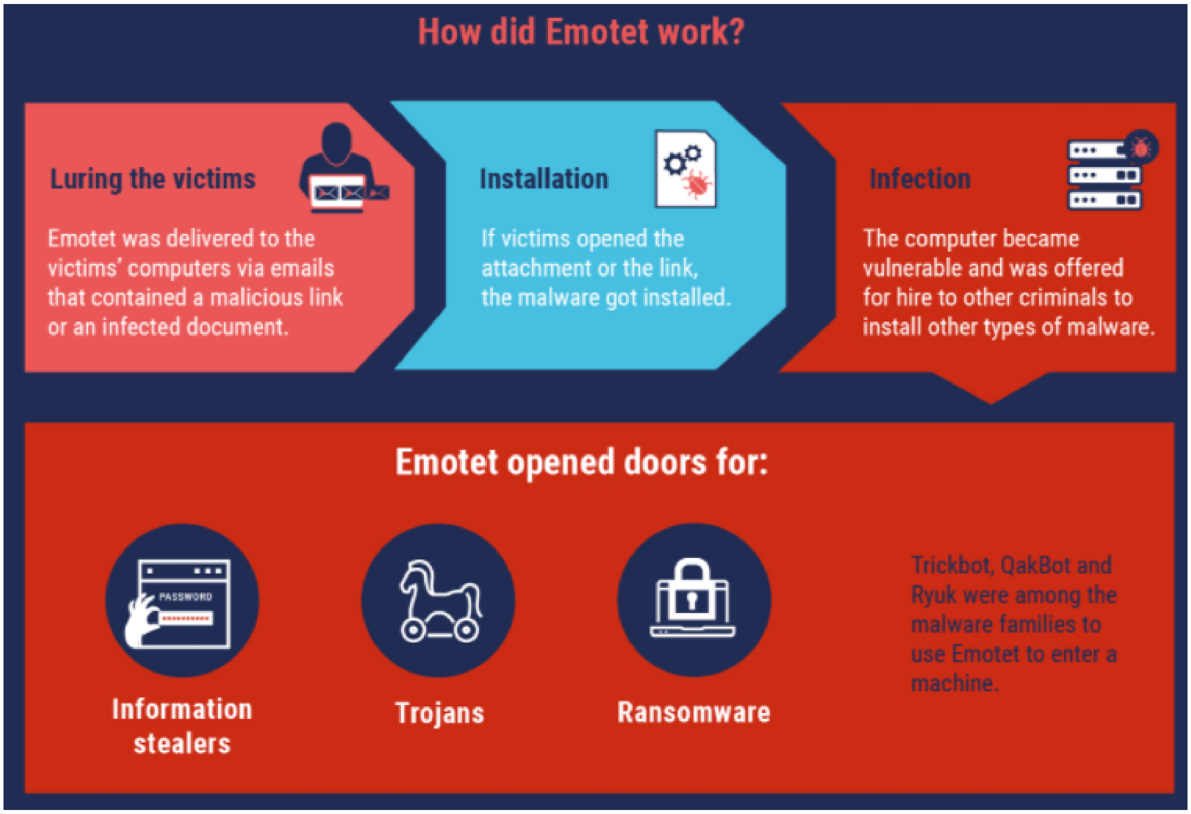
International Action Targets Emotet Crimeware

krebsonsecurity.com/2021/01/international-action-targets-emotet-crimeware

Authorities across Europe on Tuesday said they'd seized control over **Emotet**, a prolific malware strain and cybercrime-as-service operation. Investigators say the action could help quarantine more than a million **Microsoft Windows** systems currently compromised with malware tied to Emotet infections.



How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

First surfacing in 2014, Emotet began as a banking trojan, but over the years it has evolved into one of the more aggressive platforms for spreading malware that lays the groundwork for ransomware attacks.

In a statement published Wednesday morning on an action dubbed "**Operation Ladybird**," the European police agency **Europol** said the investigation involved authorities in the Netherlands, Germany, United States, the United Kingdom, France, Lithuania, Canada and Ukraine.

"The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale," Europol said. "Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware."

Experts say Emotet is a pay-per-install botnet that is used by several distinct cybercrime groups to deploy secondary malware — most notably the ransomware strain Ryuk and Trickbot, a powerful banking trojan. It propagates mainly via malicious links and attachments sent through compromised email accounts, blasting out tens of thousands of malware-laced missives daily.

Emotet relies on several hierarchical tiers of control servers that communicate with infected systems. Those controllers coordinate the dissemination of second-stage malware and the theft of passwords and other data, and their distributed nature is designed to make the crimeware infrastructure more difficult to dismantle or commandeer.

In a separate statement on the malware takeover, the Dutch National police said two of the three primary servers were located in the Netherlands.

“A software update is placed on the Dutch central servers for all infected computer systems,” the Dutch authorities wrote. “All infected computer systems will automatically retrieve the update there, after which the Emotet infection will be quarantined. Simultaneous action in all the countries concerned was necessary to be able to effectively dismantle the network and thwart any reconstruction.”

A statement from the German Federal Criminal Police Office about their participation in Operation Ladybird said prosecutors seized 17 servers in Germany that acted as Emotet controllers.

“As part of this investigation, various servers were initially identified in Germany with which the malicious software is distributed and the victim systems are monitored and controlled using encrypted communication,” the German police said.

Sources close to the investigation told KrebsOnSecurity the law enforcement action included the arrest of several suspects in Europe thought to be connected to the crimeware gang. The core group of criminals behind Emotet are widely considered to be operating out of Russia.

A statement by the National Police of Ukraine says two citizens of Ukraine were identified “who ensured the proper functioning of the infrastructure for the spread of the virus and maintained its smooth operation.”

A video released to YouTube by the NPU this morning shows authorities there raiding a residence, seizing cash and computer equipment, and what appear to be numerous large bars made of gold or perhaps silver. The Ukrainian policeman speaking in that video said the crooks behind Emotet have caused more than $2 billion in losses globally. That is almost certainly a very conservative number.

Police in the Netherlands seized huge volumes of data stolen by Emotet infections, including email addresses, usernames and passwords. A tool on the Dutch police website lets users learn if their email address has been compromised by Emotet.

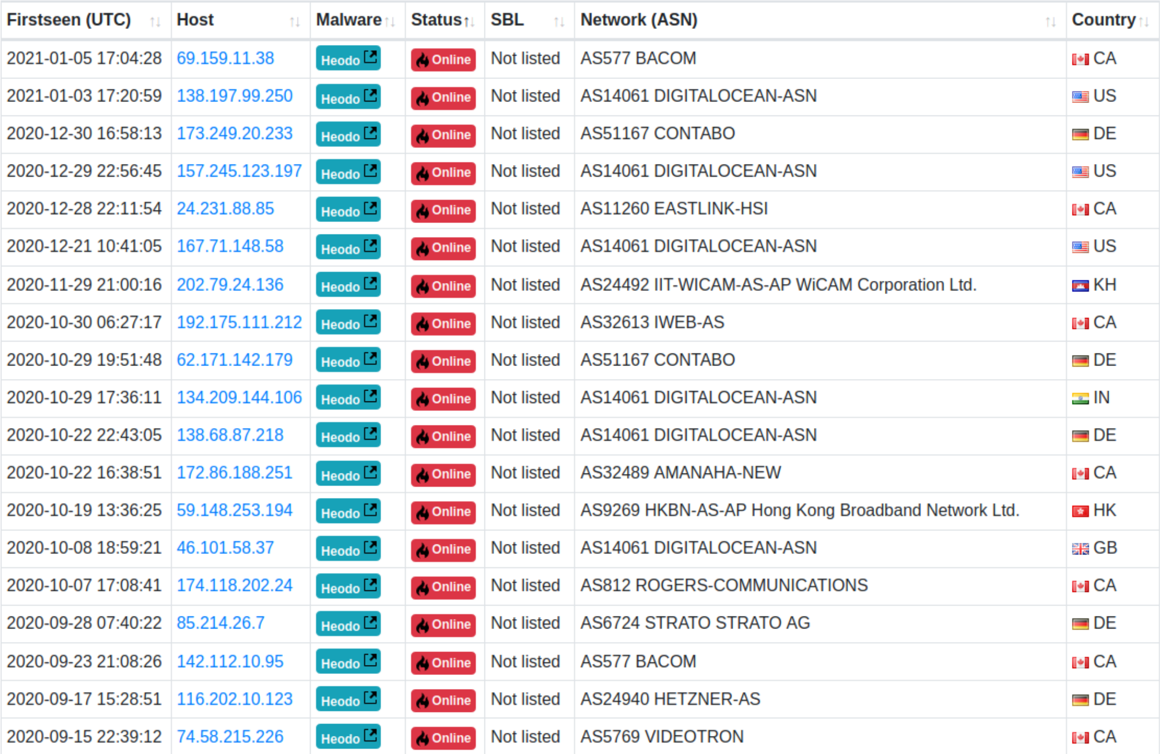
But because Emotet is typically used to install additional malware that gets its hooks deeply into infected systems, cleaning up after it is going to be far more complicated and may require a complete rebuild of compromised computers.

The **U.S. Cybersecurity & Infrastructure Security Agency** has labeled Emotet “one of the most prevalent ongoing threats” that is difficult to combat because of its ‘worm-like’ features that enable network-wide infections.” Hence, a single Emotet infection can often lead to multiple systems on the same network getting compromised.

It is too soon to say how effective this operation has been in fully wresting control over Emotet, but a takedown of this size is a significant action.

In October, **Microsoft** used trademark law to disrupt the Trickbot botnet. Around the same time, the **U.S. Cyber Command** also took aim at Trickbot. However, neither of those actions completely dismantled the crimeware network, which remains in operation today.

Roman Hüssy, a Swiss information technology expert who maintains Feodotracker — a site that lists the location of major botnet controllers — told KrebsOnSecurity that prior to January 25, some 98 Emotet control servers were active. The site now lists 20 Emotet controllers online, although it is unclear if any of those remaining servers have been commandeered as part of the quarantine effort.



Firstseen (UTC)	Host	Malware	Status	SBL	Network (ASN)	Country
2021-01-05 17:04:28	69.159.11.38	Heodo	Online	Not listed	AS577 BACOM	CA
2021-01-03 17:20:59	138.197.99.250	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	US
2020-12-30 16:58:13	173.249.20.233	Heodo	Online	Not listed	AS51167 CONTABO	DE
2020-12-29 22:56:45	157.245.123.197	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	US
2020-12-28 22:11:54	24.231.88.85	Heodo	Online	Not listed	AS11260 EASTLINK-HSI	CA
2020-12-21 10:41:05	167.71.148.58	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	US
2020-11-29 21:00:16	202.79.24.136	Heodo	Online	Not listed	AS24492 IIT-WICAM-AS-AP WiCAM Corporation Ltd.	KH
2020-10-30 06:27:17	192.175.111.212	Heodo	Online	Not listed	AS32613 IWEB-AS	CA
2020-10-29 19:51:48	62.171.142.179	Heodo	Online	Not listed	AS51167 CONTABO	DE
2020-10-29 17:36:11	134.209.144.106	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	IN
2020-10-22 22:43:05	138.68.87.218	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	DE
2020-10-22 16:38:51	172.86.188.251	Heodo	Online	Not listed	AS32489 AMANAHA-NEW	CA
2020-10-19 13:36:25	59.148.253.194	Heodo	Online	Not listed	AS9269 HKBN-AS-AP Hong Kong Broadband Network Ltd.	HK
2020-10-08 18:59:21	46.101.58.37	Heodo	Online	Not listed	AS14061 DIGITALOCEAN-ASN	GB
2020-10-07 17:08:41	174.118.202.24	Heodo	Online	Not listed	AS812 ROGERS-COMMUNICATIONS	CA
2020-09-28 07:40:22	85.214.26.7	Heodo	Online	Not listed	AS6724 STRATO STRATO AG	DE
2020-09-23 21:08:26	142.112.10.95	Heodo	Online	Not listed	AS577 BACOM	CA
2020-09-17 15:28:51	116.202.10.123	Heodo	Online	Not listed	AS24940 HETZNER-AS	DE
2020-09-15 22:39:12	74.58.215.226	Heodo	Online	Not listed	AS5769 VIDEOTRON	CA

A current list of Emotet control servers online. Source: Feodotracker.abuse.ch

Further reading: Team Cymru on taking down Emotet