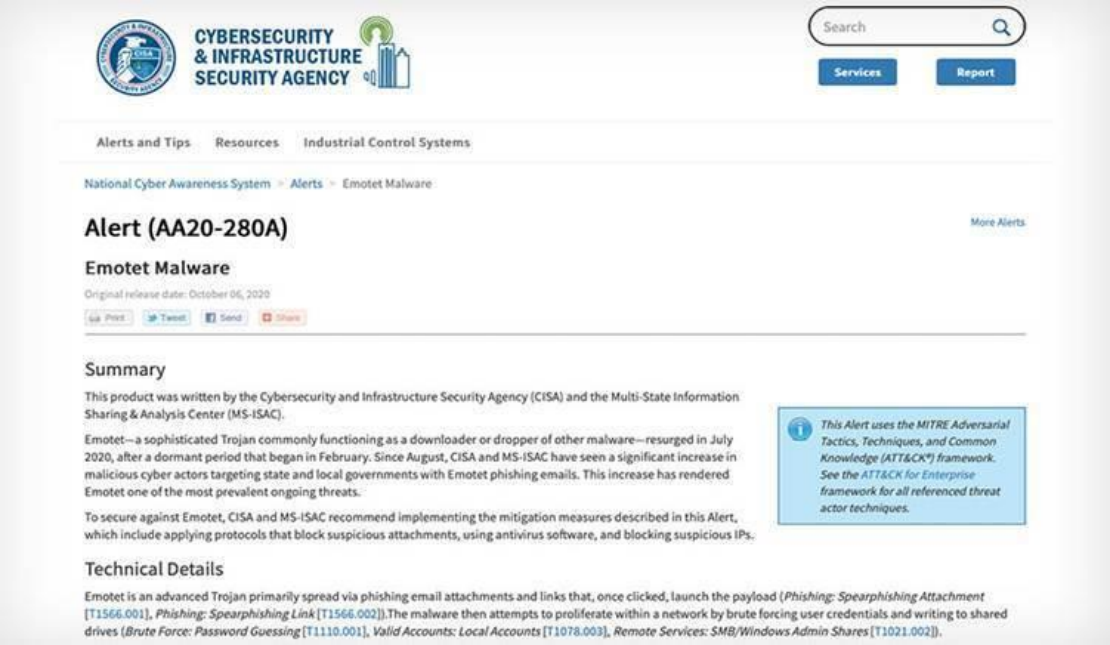
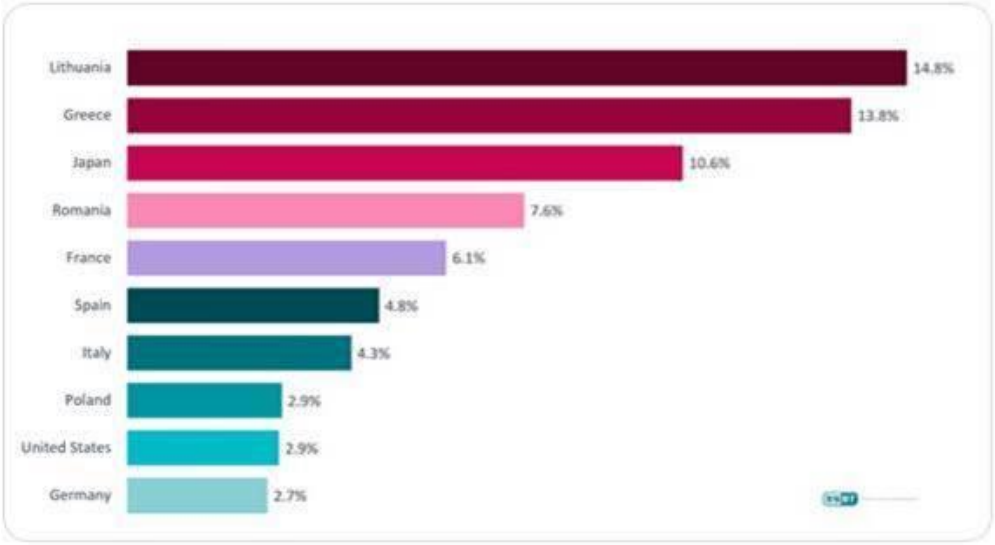
Description:

One week ago, US CISA issued a warning on eminent attack by Emotet botnet against US government sites [1].



Since Wednesday 14/10/2020 Emotet botnet has indeed returned after nearly two weeks and it came back hard. Neutrify has received alerts on 400+ e-mails, which were blocked by Security solutions on multiple customers. Some of the blocked e-mails were replies to legit e-mails by associates of our customers. We presume that these associates have either been hacked by the botnet [2].

ESET confirmed today what Neutrify is seeing; ESET team published in Twitter that Emotet is currently targeting users in 5 countries including Greece and that it is hitting these countries hard.



ESET also mentions that the emails typically consist of stolen legitimate communication and generic short lure by the operators such as “Please see enclosed document” [3].

Since Emotet botnet attack is continuing at the same pace today Neutrify recommends you stay on alert.

Mitigations:

- Issue a global alert for all your users.
- Alert your users on the campaign and instruct to be cautious (**No e-mails containing attachments or curious links even from known associates are to be trusted).**
- Block email attachments commonly associated with malware, such as DLL and EXE.
- Block email attachments, such as zip files, that cannot be scanned by antivirus software.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Implement the Domain-Based Message Authentication, Reporting and Conformance, or DMARC, validation system for emails.
- Enforce multifactor authentication.

References:

[1] https://www.govinfosecurity.com/cisa-warns-emotet-attacks-against-government-agencies-a-15130
[2] https://twitter.com/neutrify/status/1316401518627651584
[3] https://twitter.com/ESETresearch/status/1317012885235707905?s=19