Athens 30/10/2020

NEUROSOFT ANNOUNCES THAT ITS CYBERSECURITY SOLUTION, NEUTRIFY, HAS RECEIVED AND BLOCKED NUMEROUS ALERTS ESPECIALLY DURING MID-OCTOBER, SOON AFTER THE OFFICIAL WARNING ISSUED BY THE US CISA, CONFIRMING ONCE AGAIN ITS EXPERTISE IN CYBERSECURITY.

Emotet —a sophisticated Trojan commonly functioning as a downloader or dropper of other malware as well as an information stealer— resurged recently targeting 5 countries including Greece. This recent significant increase in Emotet phishing emails, has rendered Emotet one of the most prevalent ongoing threats. The US CISA (Cybersecurity and Infrastructure Agency) has released an alert in the beginning of the month, suggesting mitigation measures, in order to warn the public about the oncoming threat.

Since Wednesday 14/10/2020 Neutrify, Neurosoft' s holistic 24/7 cybersecurity solution, has received and blocked alerts on 1000+ e-mails of multiple customers. Some of the blocked e-mails were replies legit e-mails by associates of our customers (technique known as thread hijacking). We presume and have in most cases verified that these associates have been hacked by the Emotet botnet. The e-mails utilized three techniques, in order to infect the intended targets, namely malicious masqueraded links, malicious Microsoft Word document attachments and (constantly since 29/10/2020) malicious attached encrypted zipped files.

Since Emotet botnet attack is continuing at the same pace Neutrify recommends to stay alert following the bellow steps:

• 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.