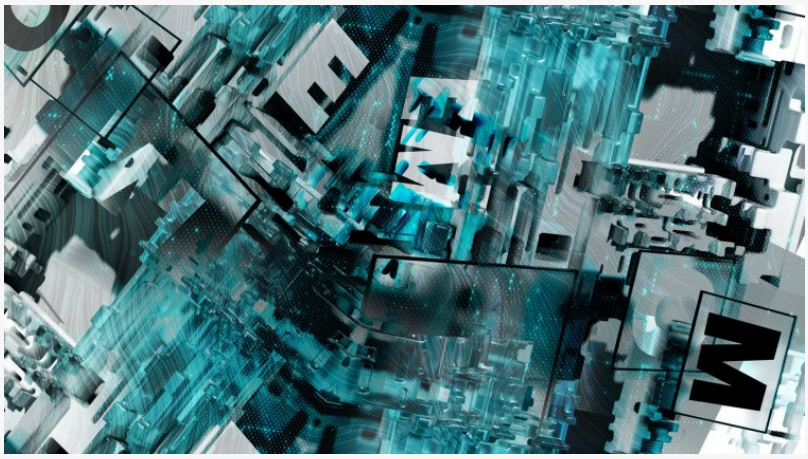
ESET Research follows the comeback of the infamous botnet Emotet, targeting mainly Japan and South Europe



DUBAI, DUBAI, UNITED ARAB EMIRATES, July 20, 2023 /EINPresswire.com/ -- ESET Research has published a summary of what happened with the Emotet botnet since its comeback after a limited takedown. Emotet is a malware family active since 2014, operated by a cybercrime group known as Mealybug or TA542. Although it started as a banking trojan, it later evolved into a botnet that became one of the most prevalent threats worldwide. In January 2021, Emotet was the target of a limited takedown as a result of an international, collaborative effort of eight countries, coordinated by Eurojust and Europol. Emotet came back to life in November 2021 and launched multiple spam campaigns with an abrupt end in April 2023. In its latest 2022-2023 campaigns, most of the attacks detected by ESET were aimed at Japan (almost half of them), Italy, Spain, Mexico, and South Africa.

"Emotet spreads via spam emails. It can exfiltrate information from, and deliver third-party malware to, compromised computers. Emotet's operators are not very picky about their targets, installing their malware on systems belonging to individuals, companies, and bigger organizations," says ESET researcher Jakub Kaloč who worked on the analysis.

Throughout late 2021 and until mid-2022, Emotet spread mainly via malicious Microsoft Word and Microsoft Excel documents with embedded VBA macros. In July 2022, Microsoft changed the game for all the malware families like Emotet and Qbot – which had used phishing emails with malicious documents as their method of distribution – by disabling VBA macros in documents obtained from the internet.

“The disabling (by authorities) of Emotet’s main attack vector made its operators look for new ways to compromise their targets. Mealybug started experimenting with malicious LNK and XLL files. However, by the time 2022 was ending, Emotet’s operators struggled to find a new attack

vector that would be as effective as VBA macros. In 2023, they ran three distinctive malspam campaigns, each testing a slightly different intrusion avenue and social engineering technique," elaborates Kaloč. "However, the shrinking size of the attacks and constant changes in the approach may suggest dissatisfaction with the outcomes".

Later Emotet embedded a lure into Microsoft OneNote, and despite warnings that this action might lead to malicious content, people tended to click on it.

After its reappearance, Emotet received multiple upgrades. The notable features were that the botnet switched its cryptographic scheme and implemented multiple new obfuscations to protect their modules. Emotet's operators have put significant effort to avoid monitoring and tracking of their botnet since they returned. They also implemented multiple new modules and improved existing modules to remain profitable.

Emotet is spread via spam emails, and people often trust those emails because it successfully uses an email thread hijacking technique. Before the takedown, Emotet used modules we call Outlook Contact Stealer and Outlook Email Stealer, capable of stealing emails and contact information from Outlook. However, because not everyone uses Outlook, post-takedown Emotet also focused on a free alternative email application – Thunderbird. Additionally, it started to use the Google Chrome Credit Card Stealer module, which steals information about credit cards stored in the Google Chrome browser.

According to ESET research and telemetry, Emotet botnets have been quiet since the beginning of April 2023, most probably due to finding a new effective attack vector. Most of the attacks detected by ESET since January 2022 until today were aimed at Japan (43%), Italy (13%), Spain (5%), Mexico (5%), and South Africa (4%).

For more technical information about Emotet, check out the blogpost "What's up with Emotet - A brief summary of what happened with Emotet since its comeback" on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant

Vistar Communications
0559724623
email us here