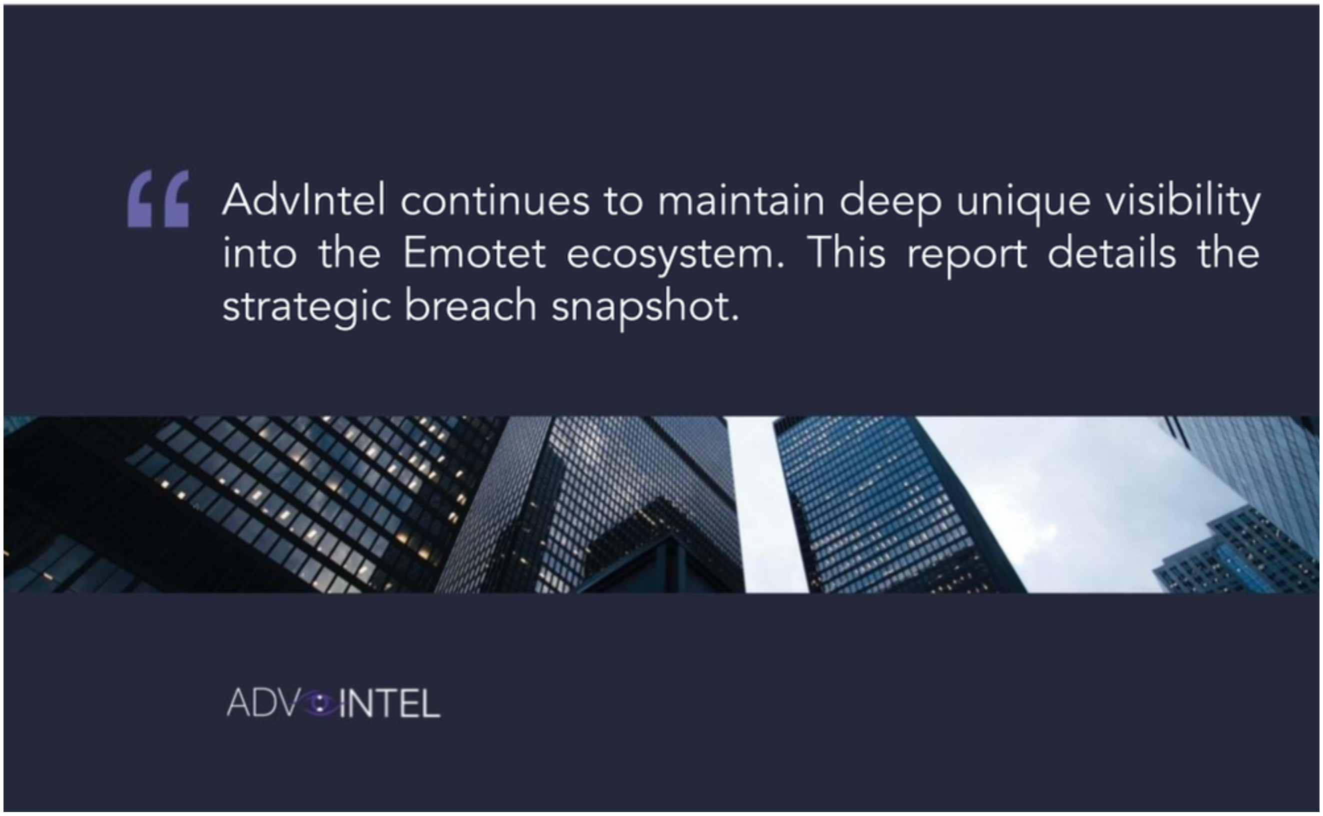
AdvIntel's State of Emotet aka "SpmTools" Displays Over Million Compromised Machines Through 2022

advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

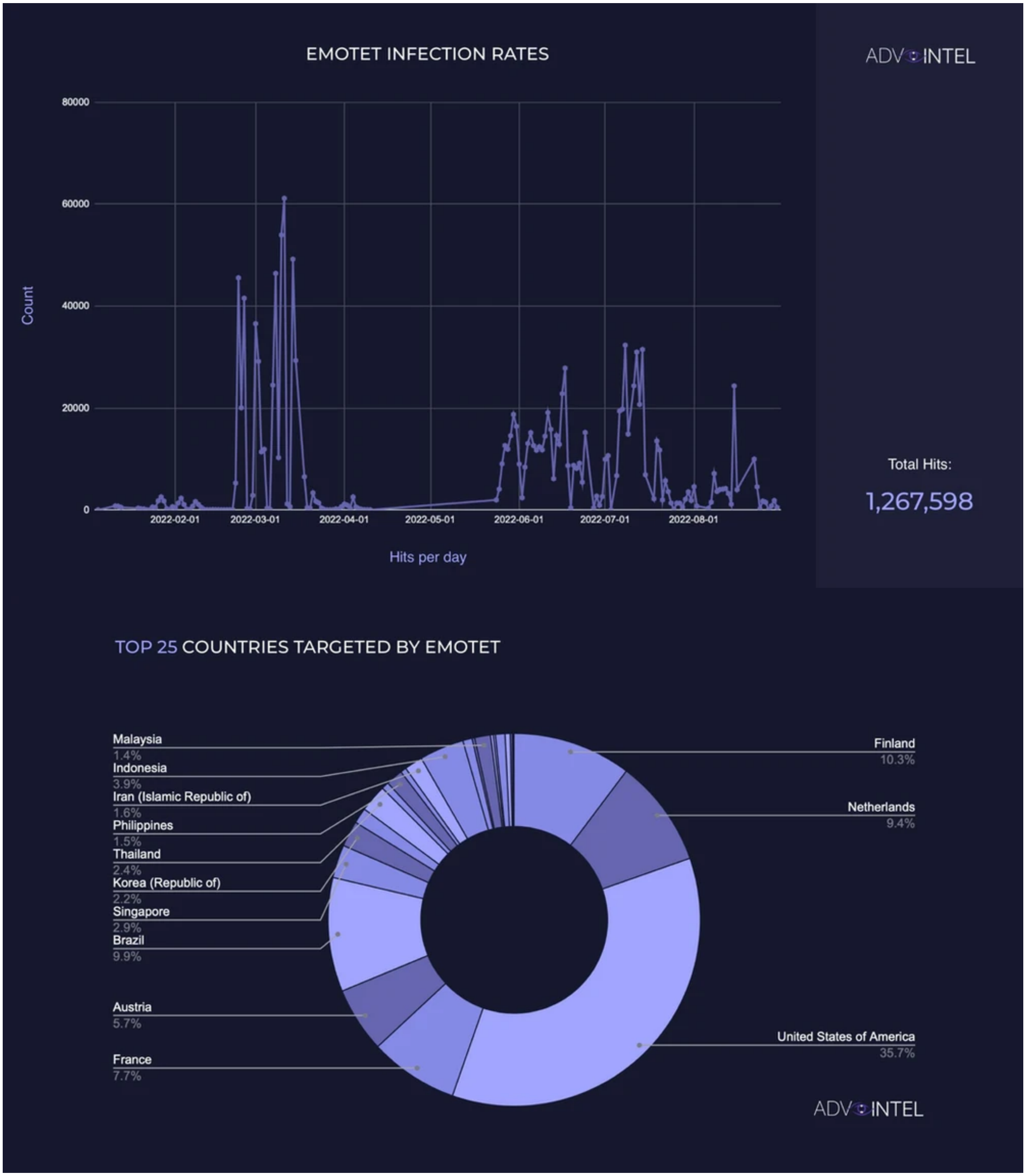
AdvIntel September 13, 2022

- Sep 13
-
- 2 min read



“ AdvIntel continues to maintain deep unique visibility into the Emotet ecosystem. This report details the strategic breach snapshot.

Throughout 2022, AdvIntel observed **1,267,598** total Emotet infections worldwide. Significant peaks in activity occurred between February/March, notably kicking off during the start of the Russian-Ukrainian conflict at the end of February, and between June/July; attributed to Emotet’s usage alongside post-Conti groups such as **Quantum** and **BlackCat**.

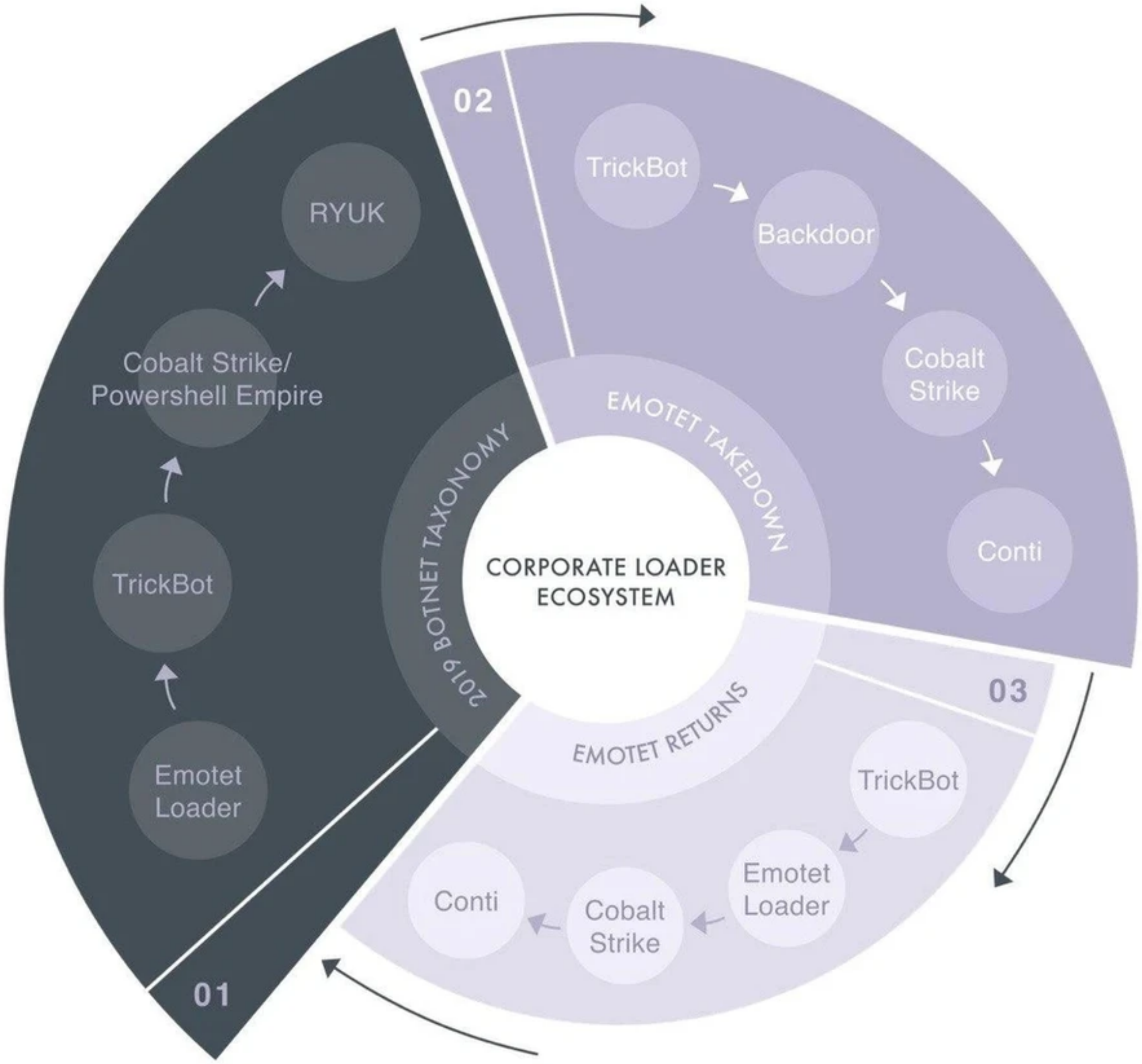


It is notable that the most Emotet-targeted country is the United States, making up 35.7% of the dataset, with Finland (10.3%), Brazil (9.9%), The Netherlands (9.4%), and France (7.7%) in the remaining top placements.

The **Emotet** botnet (also known as *SpmTool*s) has fueled major cybercriminal groups as an initial attack vector, or precursor, for numerous ongoing attacks. From November 2021 to Conti's dissolution in June 2022, Emotet was an exclusive **Conti** ransomware tool, however, the Emotet infection chain is currently attributed to **Quantum** and **BlackCat.**

Emotet is a botnet of Eastern European origin that was originally designed as a banking trojan, meant to steal sensitive banking information by intercepting internet traffic. However, updates to Emotet over time have significantly increased the threat that it poses, and it has evolved into a prominent, invasive malware loader, largely due to its ability to conduct a full infection cycle and seamlessly spread other types of malware. Since its appearance in 2014, Emotet has proved to be a consistent and highly threatening malware that has targeted individuals, companies, municipalities, and governments alike.

The observed botnet taxonomy attacker flow for Emotet is **Emotet -> Cobalt Strike -> Ransomware Operation.** What this means is that currently, the way that threat actors primarily utilize Emotet is as a dropper, or downloader for a Cobalt Strike beacon, which deploys a payload allowing threat actors to take over networks and execute ransomware operations.



An infographic depicting the progression of Emotet's place in the now-dissolved Conti's attacker flow, placed within a larger cluster of other "malware loader" and "backdoor" software. Threat actors that were previously affiliated with the Conti group continue to utilize its toolkit, which includes the Emotet botnet.

Adversarial Assessment Summary [Emotet]

Emotet [Threat Group]

Malware Type: Botnet/ Loader-as-a-Service (LaaS)

Origin: Eastern Europe

Intelligence Source: High Confidence

Functionality:

- Payload delivery

- Data exfiltration
- Credential harvesting

Distribution:

Email Phishing

Persistency: High

Infection Rate: High

Threat Assessment: Critical

Emotet Patterns [MITRE ATT&CK Framework]:

The following techniques (framed within MITRE ATT&CK categorizations) are a small sample of those utilized by Emotet (for a full list, click here).

Technique	Use
Account Discovery: Email Account	Emotet may attempt to get a listing of email addresses and accounts, or dump Exchange address lists such as global address lists (GALs).
Brute Force: Password Guessing	With no prior knowledge of legitimate credentials within the system or environment, Emotet may guess passwords to attempt access to the account.
Credentials from Password Stores: Credentials from Web Browsers	Emotet may acquire credentials from web browsers by reading files specific to the target browser.
Email Collection: Local Email Collection	Emotet may target user email on local systems to collect sensitive information.
Exfiltration Over C2 Channel	Adversaries may steal data by exfiltrating it over an existing command and control channel.
Process Injection: Dynamic-link Library Injection	Emotet may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges.

User Execution: Malicious File	Emotet may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution.

For more on Emotet botnet telemetry, please reach out to support@advintel.tech.