REPORT

DECEMBER **2025**

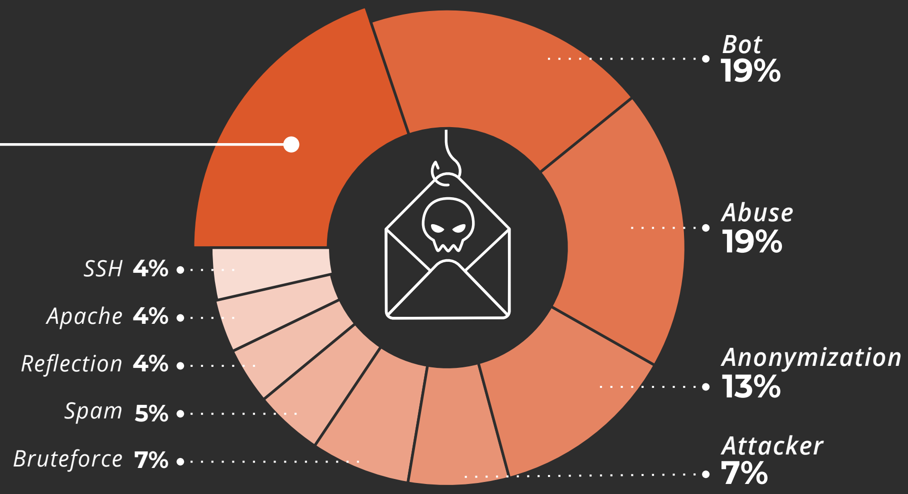
maltiverse

by LUMU

REPORT Data collected from December 1 to December 31.

Indicators by **Type of Activity**

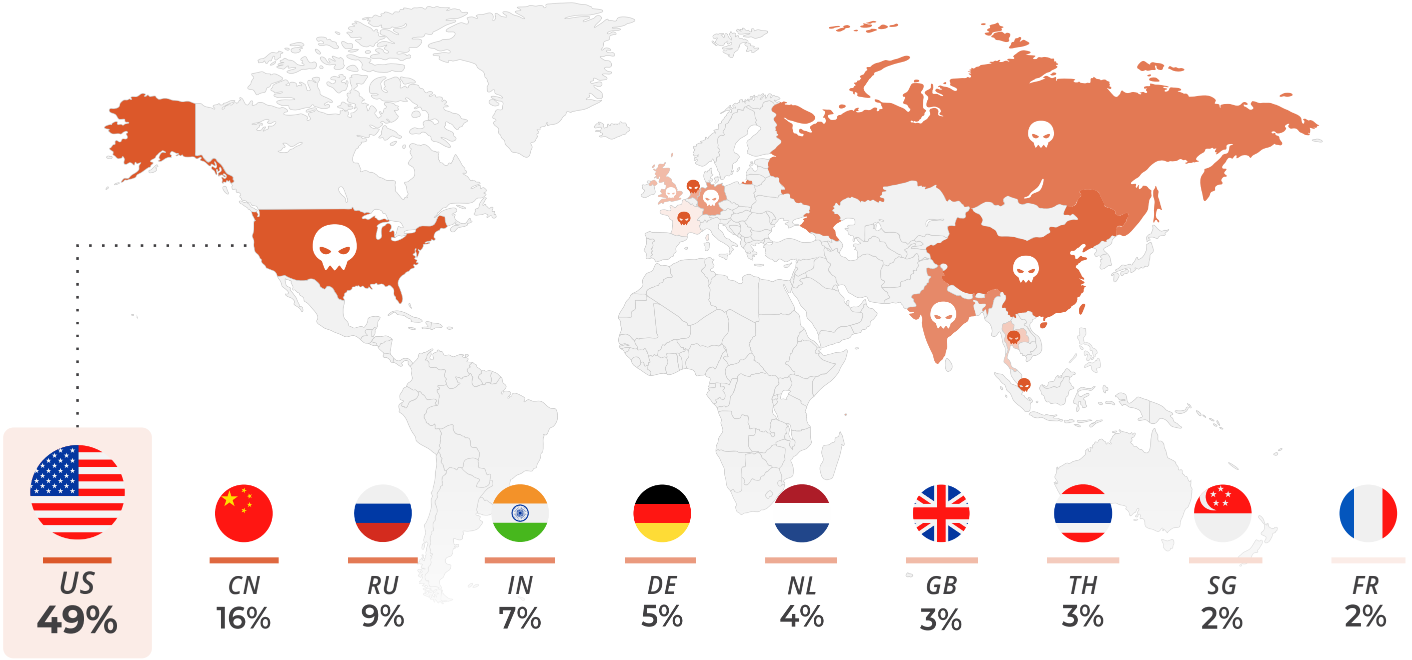
20% Phishing



Behaviors are identified through Indicators of Compromise (IoCs), which classify threats according to their nature.

Indicators by **Country**

Visual representation of the geographic concentration of detected malicious activity, which enables the analysis and prioritization of threats based on their origin.



Most active
Malware Families

Threat landscape analysis that enables the identification of the most active malware families—an essential step for defining defensive measures and effectively adjusting cybersecurity strategies.

ID: S0650
Type: *Malware*
Platforms: *Windows*
Version: *1.3*

QakBot 38.9%

Is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007.

Groups That Use This Software

G0127 / G1037 / G1046

ID: S0154
Type: *Malware*
Platforms: *Windows, Linux, macOS*
Version: *1.13*

Cobalt Strike 13.7%

Is a commercial, full-featured, remote access tool that bills itself as adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors.

Groups That Use This Software

G0129 - Mustang Panda / G0027 - Threat Group-3390 / G0050 - APT32 / G1022 - ToddyCat / G0073 - APT19 / G0037 - FIN6 / G0092 - TA505

ID: S0367
Type: *Malware*
Platforms: *Windows*
Version: *1.7*

Emotet 13.5%

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID.

Groups That Use This Software

G0102

ID: S1087
Type: *Tool*
Platforms: *Windows*
Version: *1.0*

AsyncRAT 7.4%

AsyncRAT is an open-source remote access tool originally available through the NYANxCAT Github repository that has been used in malicious campaigns.

Groups That Use This Software

G1018

ID: S0385
Type: *Malware*
Platforms: *Windows*
Version: *1.6*

njRAT 5.9%

Is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.

Groups That Use This Software

G0134 - G0043 - G0143 - G0096 - G0140 - G0078 - G1018

ID: S1207
Type: *Malware*
Platforms: *Windows*
Version: *1.0*

XLoader 5.0%

Is an infostealer malware in use since at least 2016. Previously known and sometimes still referred to as Formbook, XLoader is a Malware as a Service (MaaS) known for stealing data from web browsers, email clients and File Transfer Protocol (FTP) applications.

ID: S0332
Type: *Tool*
Platforms: *Windows*
Version: *1.3*

Remcos 4.8%

Is a commercial Trojan that is used to steal information from compromised hosts.

Groups That Use This Software

G0092 - TA505

ID: S1213
Type: *Malware*
Platforms: *Windows*
Version: *1.0*

Lumma Stealer 4.0%

DarkGate first emerged in 2018 and has evolved into an initial access and data gathering tool.

ID: S0262
Type: *Tool*
Platforms: *Windows*
Version: *2.1*

QuasarRAT 3.6%

QuasarRAT is an open-source, remote access tool that has been publicly available on GitHub since at least 2014

Groups That Use This Software

G0040 / G0140 / G0078 / G0094 / G0045 / G0135

ID: S0447
Type: *Malware*
Platforms: *Windows*
Version: *2.0*

Lokibot 3.2%

Is a widely distributed information stealer that was first reported in 2015.

Groups That Use This Software

G0083