REPORT

NOVEMBER 2025

maltiverse

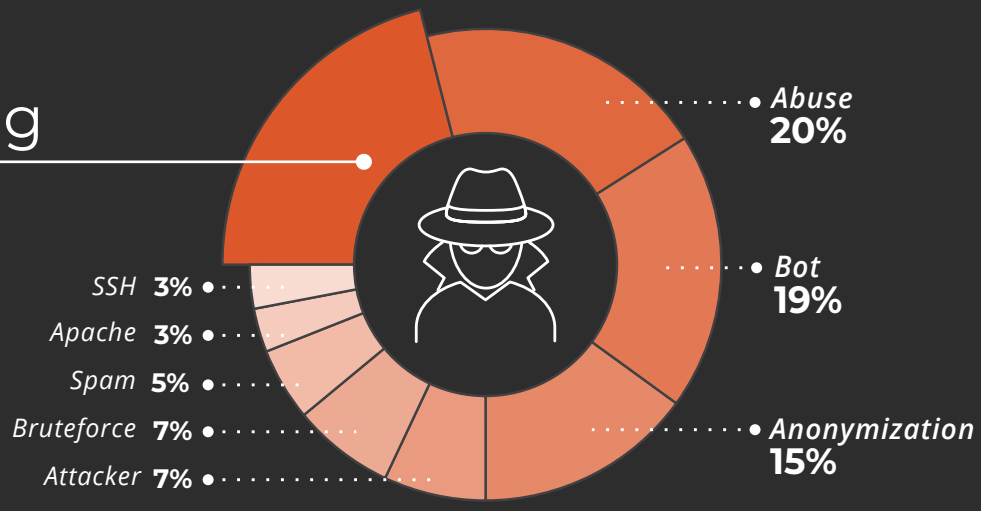
by LUMU

REPORT Data collected from November 1 to November 30.

Indicators by **Type of Activity**

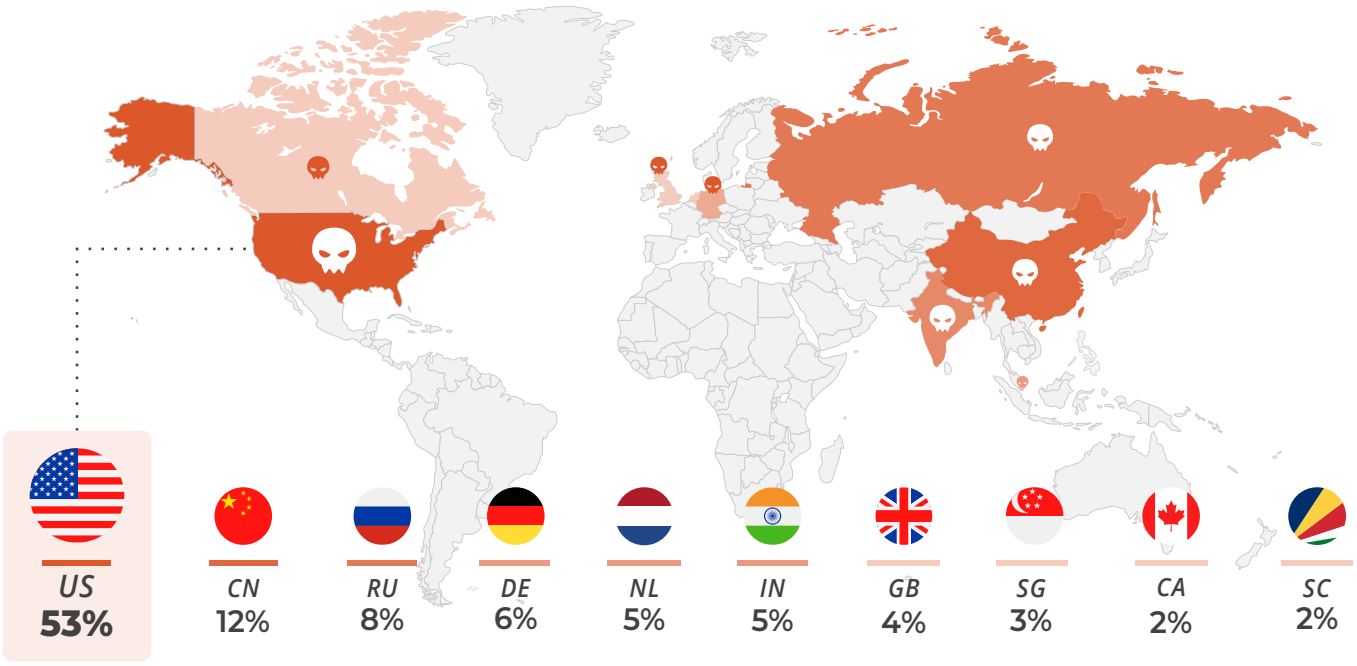
21% Phishing

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



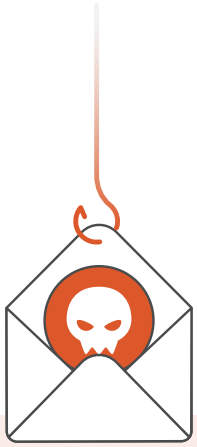
Indicators by **Country**

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: T1566
Type: *Malware*
Platforms: *Google Workspace, Linux, Office 365, SaaS, Windows, macOS*
Version: *2.5*

Phishing 94.7%

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering.

Procedure Examples

G0001 - Axiom / G0115 - GOLD SOUTHFIELD / S0009 - Hikit / S1073 - Royal

ID: S0650
Type: *Malware*
Platforms: *Windows*
Version: *1.2*

QakBot 2.3%

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

Groups That Use This Software

G0127 - TA551

ID: S0154
Type: *Malware*
Platforms: *Windows, Linux, macOS*
Version: *1.12*

Cobalt Strike 0.7%

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 0.5%

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: *Malware*
Platforms: *Windows*
Version: *1.0*

DarkGate 0.4%

DarkGate first emerged in 2018 and has evolved into an initial access and data gathering tool associated with various criminal cyber operations.

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

njRAT 0.4%

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 0.3%

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 0.3%

Remcos is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security. Remcos has been observed being used in malware campaigns.

Groups That Use This Software
G0140, G0047, G0078

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

Lumma Stealer 0.3%

Is an information stealer malware family in use since at least 2022. Lumma Stealer is a Malware as a Service (MaaS) where captured data has been sold in criminal markets to Initial Access Brokers.