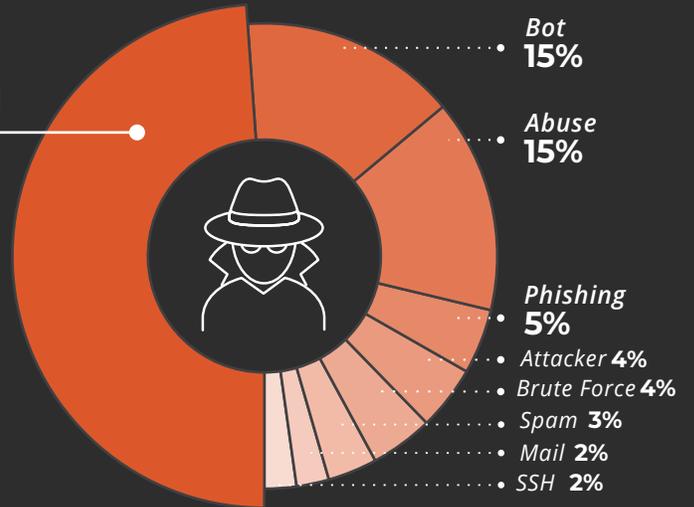# REPORT
AUGUST 2025

maltiverse
by LUMU

Indicators by
Type of Activity

## 49% Anonymization

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

Bot 15%
Abuse 15%
Phishing 5%
Attacker **4%**
Brute Force **4%**
*Spam* **3%**
Mail **2%**
SSH **2%**

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.

US 45% **RU 14%** **CN 13%** **SG 5%** **DE 5%** **GB 5%** **IN 4%** **UA 3%** **CA 3%** **ZA 3%**
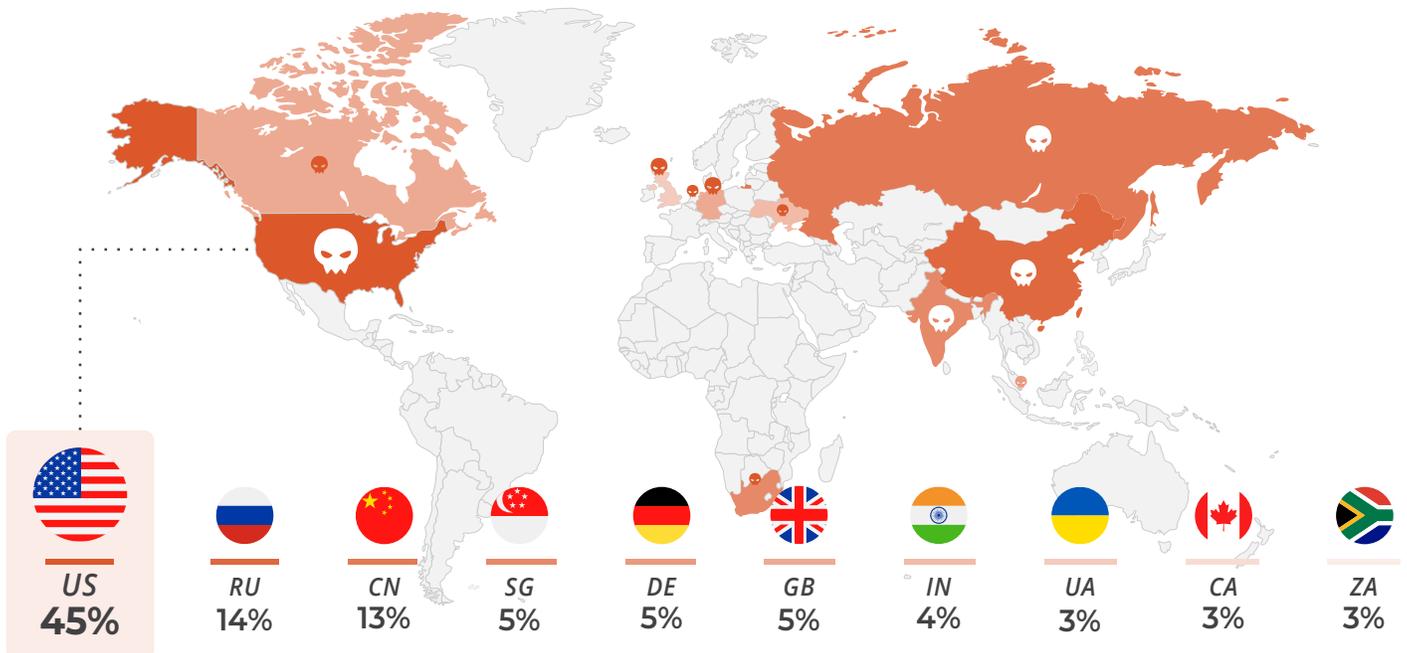
Most active
Malware Families

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.
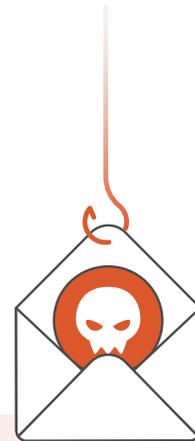
ID: T1566

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

Phishing 86%

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 5%

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: S0453

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

Pony 3%

Is a credential stealing malware, though it has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.

ID: S0447

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

Lokibot 2%

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

Groups That Use This Software

G0083

ID: S0154

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

Cobalt Strike 2%

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-
G0073 - APT19 / G0037 - FIN6 / G0092 - TA505

ID: S0344

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

Azorult 1%

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 1%

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.

ID: S1087

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

DarkGate 1%

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

ID: S0385

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

njRAT 1%

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