THREAT INTELLIGENCE REPORT MARCH 2026

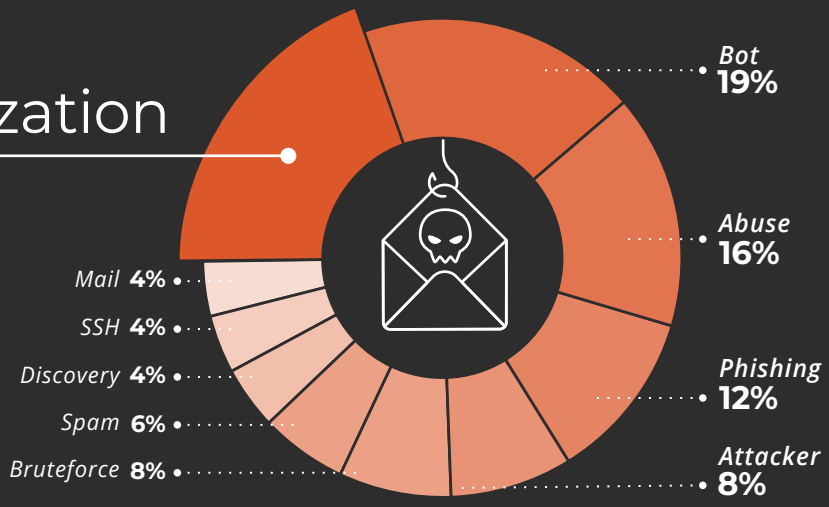
LUMU

REPORT Data collected from March 1 to March 31.

Indicators by **Type of Activity**

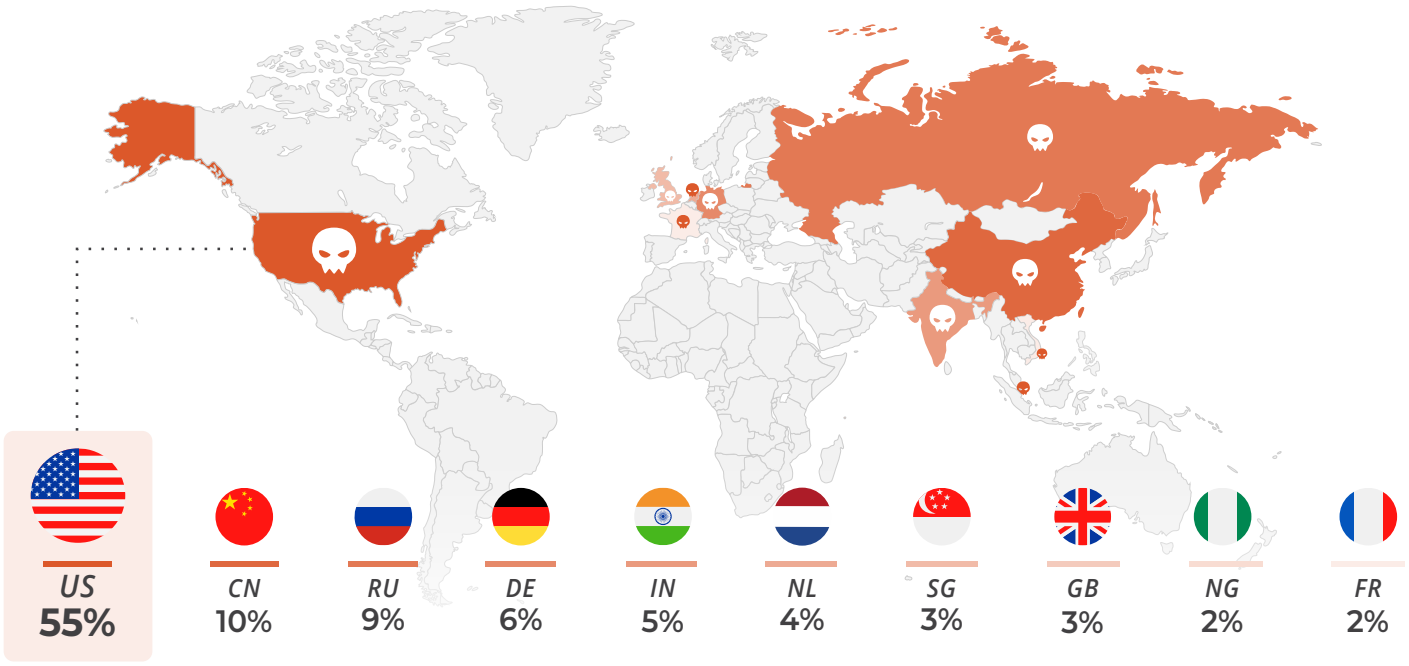
20% Anonymization

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.



REPORT Data collected from March 1 to March 31.

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

Cobalt Strike 54.9%

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

G1053 / G1046 / G0129 / G0027 / G0050 / G1022 / G0073 / G0037 / G0092 / G0052 / G0079 / G1040 G1006 / G0046 / G1020 / G0096 / G0045 / G0143 / G0080 / G0034 / G1043 / G0065 / G0016 / G1021 G0067 / G1014 / G0114 / G0119 / G0102

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

QakBot 17.8%

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

AsyncRAT 5.2%

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

Emotet 5.0%

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

Remcos 3.8%

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

Groups That Use This Software

G0140 / G0047 / G0078

ID: S0331
Type: *Malware*
Platforms: *Windows*
Version: *1.3*

Agent Tesla 3.3%

Agent Tesla is a spyware Trojan written for the .NET framework that has been observed since at least 2014.

Groups That Use This Software

G0083 / G1018

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

njRAT 2.9%

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 2.6%

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: S0032
Type: *Malware*
Platforms: *Windows, macOS*
Version: *3.3*

gh0st RAT 2.4%

gh0st RAT is a remote access tool (RAT). The source code is public and it has been used by multiple groups.

Groups That Use This Software

G0062 / G0096 / G0011 / G0001 / G0027 / G0094 / G0065 / G0026 / G0126 / G0138 / G1023

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

Lumma Stealer 1.8%

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