THREAT INTELLIGENCE REPORT

APRIL 2026

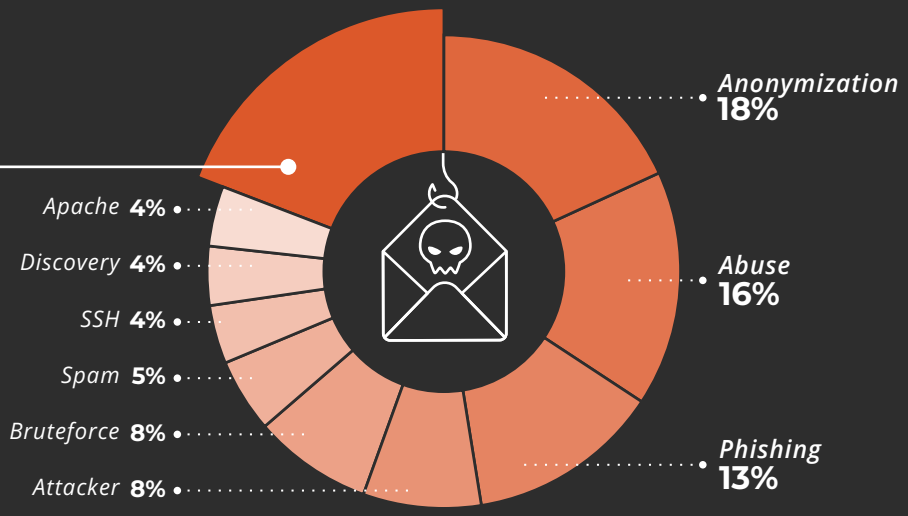
LUMU

REPORT Data collected from April 1 to April 30.

Indicators by **Type of Activity**

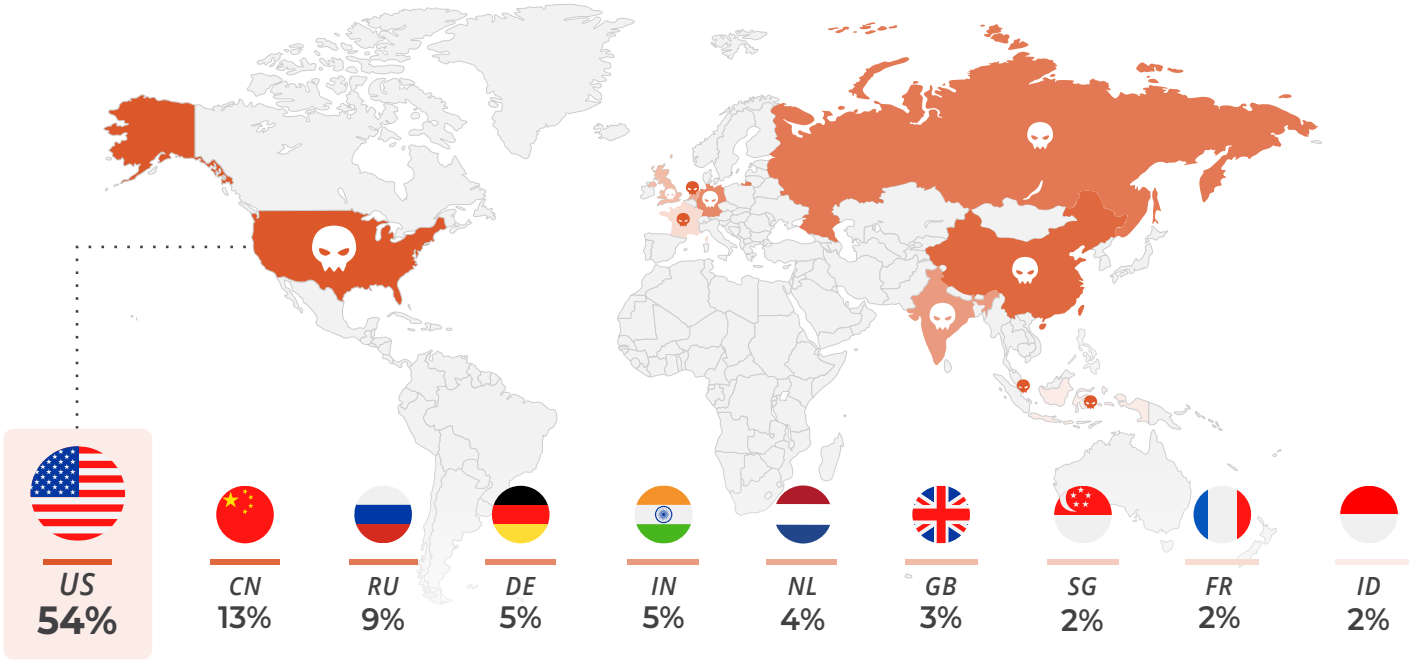
19% Bot

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 April 1 to April 30.

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: *Linux, macOS, Windows*
Version: *1.14*

Cobalt Strike 52.12%

Commercial adversary simulation and remote access framework widely used for post-exploitation.

Groups That Use This Software
G1054 \ 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 14.28%

Modular banking trojan that evolved into an information stealer and ransomware delivery mechanism.

Groups That Use This Software
G0127 \ G1037 \ G1046

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

AsyncRAT 7.97%

Open-source remote access tool that has been repurposed in malicious campaigns.

Groups That Use This Software
G1018 \ G0099 \ G1054

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

Emotet 5.92%

Modular malware mainly used as a downloader for other malware families.

Groups That Use This Software
G0102

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

Agent Tesla 5.71%

.NET spyware trojan observed since at least 2014.

Groups That Use This Software
G0083 \ G1018

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

XLoader 4.02%

Infostealer malware, formerly known as Formbook, offered as MaaS and focused on browser, email, and FTP theft.

ID: S0332
Type: *Tool*
Platforms: *Windows*
Version: *1.4*

Remcos 3.07%

Closed-source remote control and surveillance tool that has also been used in malicious operations.

Groups That Use This Software
G0140 \ G0047 \ G0099 \ G0078

ID: S0385
Type: *Malware*
Platforms: *Windows*
Version: *1.7*

njRAT 2.70%

Remote access tool first seen in 2012 and used by multiple threat actors, especially in the Middle East.

Groups That Use This Software
G0099 \ G0134 \ G0043 \ G0143 \ G0096 \ G0140 \ G0078 \ G1018

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

gh0st RAT 2.26%

Publicly available remote access tool whose code has been used by many groups.

Groups That Use This Software
G0062 \ G0096 \ G0011 \ G0001 \ G0027 \ G0094 \ G0065 \ G0026 \ G0126 \ G0138 \ G1023

ID: S0051
Type: *Malware*
Platforms: *Windows*
Version: *1.3*

MiniDuke 1.94%

Multi-component malware used by APT29 between 2010 and 2015 for download and backdoor activity.

Groups That Use This Software
G0016