THREAT INTELLIGENCE REPORT MAY 2026

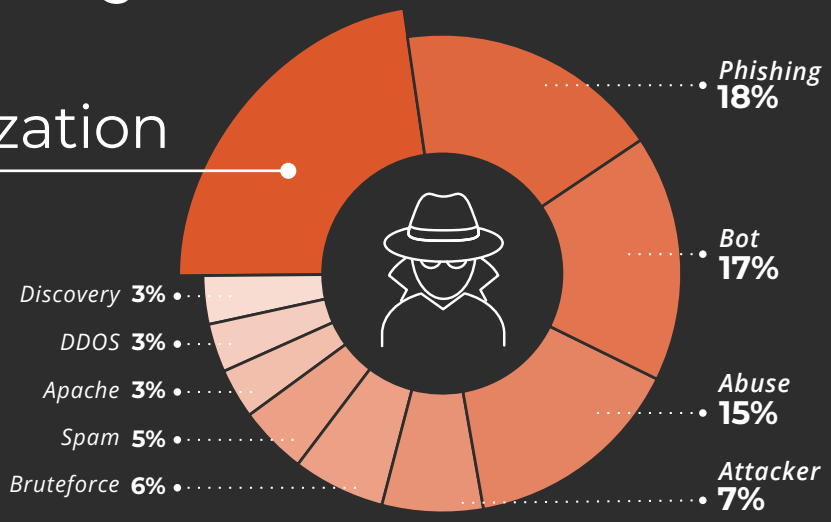
LUMU

REPORT Data collected from May 1 to May 31.

Indicators by **Type of Activity**

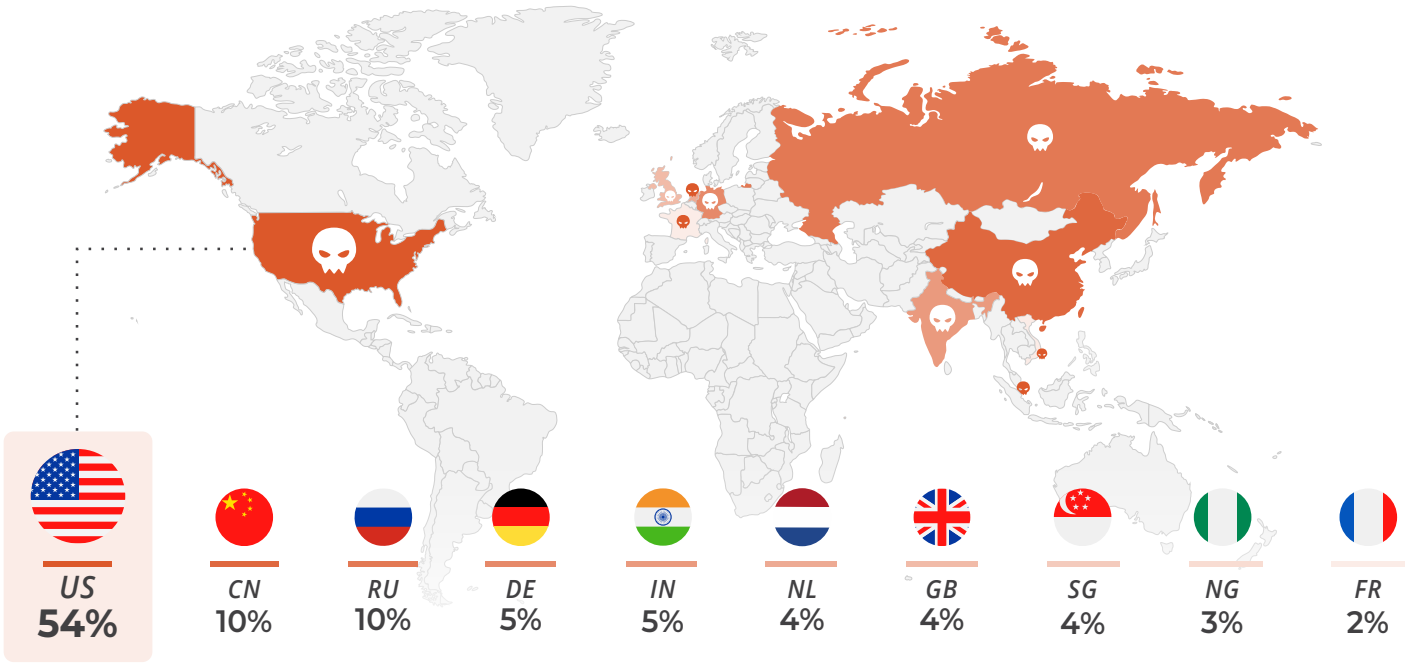
23% Anonymization

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 May 1 to May 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: *Tool*
Platforms: *Windows, Linux, macOS*
Version: *1.14*

Cobalt Strike 60.5%

A commercial remote access tool for adversary simulation that provides interactive post-exploitation capabilities covering the full range of ATT&CK tactics.

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 12.1%

A modular banking trojan used by financially-motivated actors since 2007 that has evolved from an information stealer into a delivery agent for ransomware.

Groups That Use This Software

G0127 / G1037 / G1046

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

AsyncRAT 9.4%

An open-source remote access tool that can be deployed via batch script and used for keylogging, screen capture, and process discovery.

Groups That Use This Software

G1018 / G0099 / G1054

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

XLoader 4.1%

XLoader is an infostealer malware and Malware as a Service (MaaS) known for stealing data from web browsers, email clients, and FTP applications.

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

Remcos 2.7%

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

Groups That Use This Software

G0140 / G0047 / G0099 / G0078

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

Agent Tesla 2.6%

A spyware Trojan written for the .NET framework that performs keylogging, credential theft, and system reconnaissance.

Groups That Use This Software

G0083 / G1018

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

njRAT 2.4%

njRAT is a remote access tool first observed in 2012 that has been used by threat actors to steal credentials, capture screenshots, and perform remote desktop access on infected systems.

Groups That Use This Software

G0099 / G0134 / G0043 / G0143 / G0096 / G0140 / G0078 / G1018

ID: S0198
Type: *Malware*
Platforms: *Windows, Linux, macOS*
Version: *1.6*

NETWIRE 2.1%

NETWIRE is a multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012 to conduct surveillance and control compromised systems.

Groups That Use This Software

G0089 / G0064 / G0083 / G1018

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

Emotet 2.1%

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

Groups That Use This Software

G0102

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

MiniDuke 1.6%

MiniDuke is malware used by APT29 consisting of multiple downloader and backdoor components that communicate via HTTP, HTTPS, Twitter, and Google Search.

Groups That Use This Software

G0016