REPORT MAY 2025

maltiverse

by LUMU

Content

RESEARCH ARTICLE

REPORT

NEWS

SERVICES

RESEARCH ARTICLE

Advisory Alert: Lumma Stealer Rebounds After Takedown

Antonio Gómez

In May 2025, an international operation led by Microsoft, the FBI, and Europol dealt what appeared to be a decisive blow to Lumma Stealer, an info-stealing malware that had compromised over 394,000 Windows systems in just three months. Authorities seized 2,300 malicious domains and disrupted its command-and-control (C2) infrastructure. However, the malware quickly showed remarkable resilience, resurfacing within days. On May 28 and 29 alone, more than 450 new indicators of compromise (IoCs) were recorded daily—surpassing pre-takedown levels.

Lumma's persistence is rooted in a robust architecture built on four pillars: a Malware as a Service (MaaS) model that operates like a franchise, with affiliates paying monthly fees; decentralized affiliates who run independent campaigns; redundant infrastructure using Telegram bots, Steam profiles, and Cloudflare proxies; and constant code evolution that includes advanced evasion techniques like process injection and obfuscation.

While not officially confirmed, multiple clues suggest Russian or Eastern European origins, including the developer "Shamel," registrar activity, and linked email accounts.

Lumma relies heavily on top-level domains like .top, .shop, and .run, and leverages infrastructure from providers like Cloudflare and DigitalOcean, showcasing its adaptability. Its covert behavior reveals a harsh reality: EDR alone is not enough. A more comprehensive approach is required—Threat Intelligence to anticipate attacks and Network Detection and Response (NDR) to catch malicious traffic that evades endpoint controls.

Lumu recommends combining EDR, NDR, and real-time threat intelligence, hardening endpoints, and ensuring teams are prepared for incidents. The key message is clear: adapt or be outmaneuvered. Lumma is a case study in how cybercrime evolves—and demands a layered, modern defense strategy.

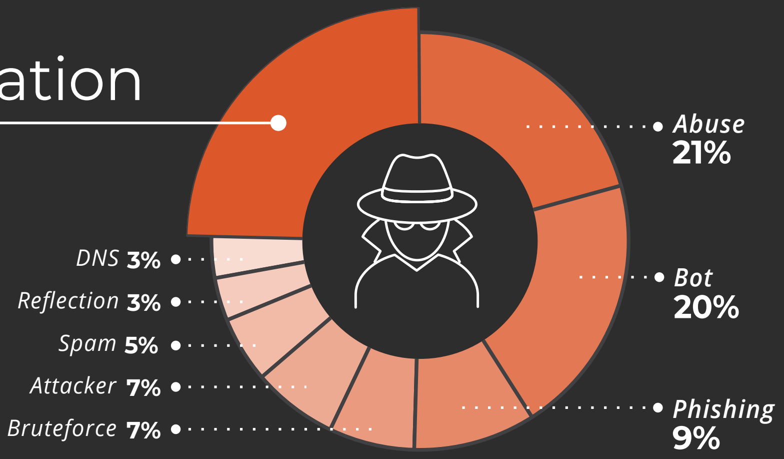
Read the full article here.

REPORT Data collected from May 1 to May 31.

Indicators by **Type of Activity**

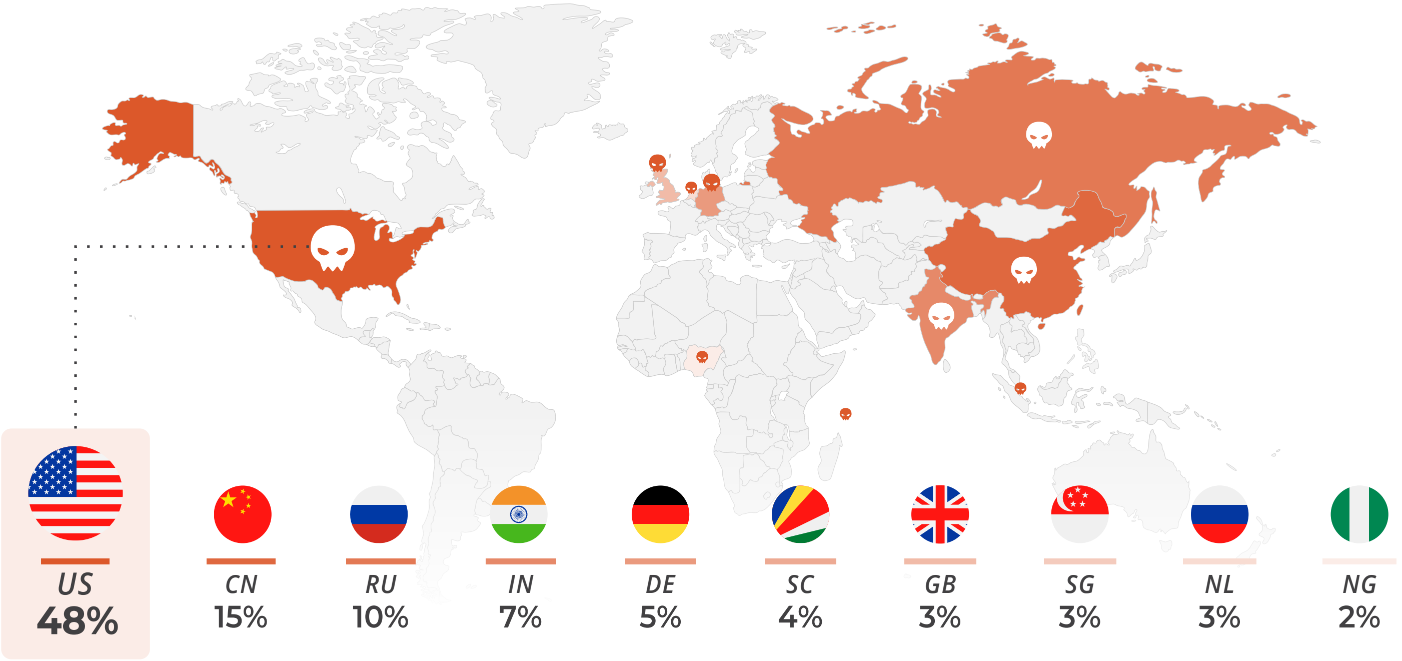
25% Anonymization

Behaviors identified through Indicators of Compromise (IoCs), which allow threats to be classified according to their nature.



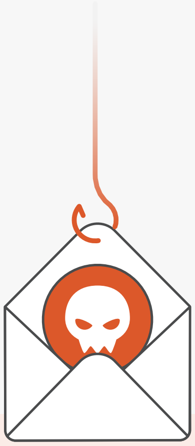
Indicators by **Country**

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 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 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: 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 associated with various criminal cyber operations.

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: S0332

Type: *Tool*

Platforms: *Windows*

Version: *1.3*

Remcos 1%

Is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security.

Groups That Use This Software

G0140 - G0078

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

NEWS

Scattered Spider Hackers **Expand Operations from UK to US Retailers**

The hacking group known as Scattered Spider, previously linked to cyberattacks on UK retailers like Marks & Spencer, Co-op, and Harrods, is now targeting US retailers. Google's Mandiant cybersecurity unit reports that the group employs social engineering tactics, such as impersonating employees to gain system access. Scattered Spider, composed of native English speakers from the UK, US, and Canada, often recruits young individuals through platforms like Discord and Telegram. The UK's National Cyber Security Centre has issued warnings, urging companies to strengthen their IT support procedures to counter these sophisticated attacks.

Read the full history

India Tightens Surveillance Camera Regulations Amid Espionage Concerns

India has implemented stringent regulations requiring manufacturers of internet-connected CCTV cameras to submit hardware, software, and source code for government lab testing. Effective from April 9, 2025, the policy aims to mitigate espionage risks, particularly from Chinese firms like Hikvision and Dahua, which hold significant market shares. The move has faced opposition from global surveillance companies citing potential supply disruptions due to limited testing infrastructure. Despite lobbying efforts, the Indian government remains firm, emphasizing national security and the need for tamper-proof, secure surveillance equipment. As of May 28, only 35 models have passed the new testing requirements, highlighting bottlenecks in the approval process.

Read the full history

EU Expresses Solidarity with Czech Republic After Cyberattack Attributed to China

The European Union has expressed solidarity with the Czech Republic following a cyberattack targeting its Ministry of Foreign Affairs, attributed to China's APT31 group. EU foreign policy chietf Kaja Kallas condemned the attack as a violation of international norms in cyberspace. The EU highlighted a growing trend of cyberattacks originating from China against its member states and urged China to take effective measures to prevent such incidents. Kallas emphasized that states must not allow their territory to be used for malicious cyber activities and warned that the EU is prepared to take additional actions to deter such behavior.

Read the full history

Marks & Spencer Faces £300 Million Loss Due to Cyberattack

Marks & Spencer (M&S) is grappling with the aftermath of a "highly sophisticated and targeted" cyberattack, resulting in an estimated £300 million loss in operating profit. The attack disrupted online services, forced manual operations for inventory management, and led to stock shortages. M&S confirmed that some customer data, including names, addresses, and birth dates, were compromised. The company anticipates that online services will remain affected until July and is working with cybersecurity experts to manage the crisis.

Read the full history

[82]
[82]
#include <stdio.h>
int main() {
int number1, number2, sum;
printf("Enter two integers: ");
scanf("%d %d", &number1, &number2);
// calculating sum
sum = number1 + number2;
[82]

UK Sees Surge in 'Remote Purchase' Fraud as Customers Tricked into Sharing Passcodes

In 2024, the UK experienced a significant increase in "remote purchase" fraud, reaching nearly 2.6 million cases, or over 7,000 incidents daily. Fraudsters exploit stolen or deceived details, especially one-time passcodes (OTPs), to make unauthorized online purchases. While total financial fraud losses remained around £1.2 billion, confirmed fraud cases rose by 12% to over 3.3 million. UK Finance urges the government to treat financial fraud as a national security threat, highlighting the need for increased public awareness and stronger security measures.

Read the full history

China Accuses Taiwan of Cyberattack on Technology Company

Chinese authorities in Guangzhou have accused Taiwan's government of orchestrating a cyberattack on an unnamed technology company. The attack is reportedly the work of a foreign hacker organization allegedly backed by Taiwan's ruling Democratic Progressive Party (DPP). The claim is based on an initial investigation conducted by local police in Guangdong province. As of now, Taiwan's Mainland Affairs Council has not responded to requests for comment. This accusation further strains the already tense cross-strait relations between China and Taiwan.

Read the full history

maltiverse
by LUMU

Services

CTI for SOAR

SOAR platforms streamline task coordination and automation across users and tools. Maltiverse enriches this process with IoC context and classifications, enabling playbooks that improve decision-making effectiveness.

CTI for SIEM

A SIEM correlates logs, using user and entity behavior analysis to identify threats and send alerts. While it is effective, it can generate too many alerts, resulting in alert fatigue.

CTI for Firewalls

Firewalls are barriers between private networks and the Internet. Maltiverse delivers threat intelligence feeds that sync with firewalls to secure outbound connections to C2 servers and malware distribution sites.

The Enteprise Plan offers a **14-day free trial for Enterprise Customers**
Upgrade your detection capabilities

Start 14 Days Trial

Actionnable Threat Inteligence

Maltiverse Intelligence Plan provides a cloud based solution to delegate the collection, classification, filtering and delivery of Indicators of Compromise. It provides a powerful baseline protection aggregated from more than 100 different public and private intelligence sources that can be integrated in less than 30 minutes. Forget about setup and maintenance, delegate to highly skilled cybersecurity professionals at Maltiverse.

Start 14 Days Trial

Threat Intelligence Platform

Maltiverse Platform is a cloud-based TIP that seamlessly integrates your intelligence from MISP and other sources, enriching and filtering out false positives to ensure your data is ready for delivery to your security devices, such as SIEMs, SOARs, Firewalls, or EDRs. Beyond leveraging your own intelligence, Maltiverse also offers industry-leading intelligence feeds, delivering the most powerful and reliable Threat Intelligence available in the market.

Start 14 Days Trial