
maltiverse
Actionable Threat Intelligence
REPORT MAR
2025
www.maltiverse.com

CONTENT

maltiverse
Actionable Threat Intelligence

maltiverse
Actionable Threat Intelligence

news

Warning about Medusa ransomware

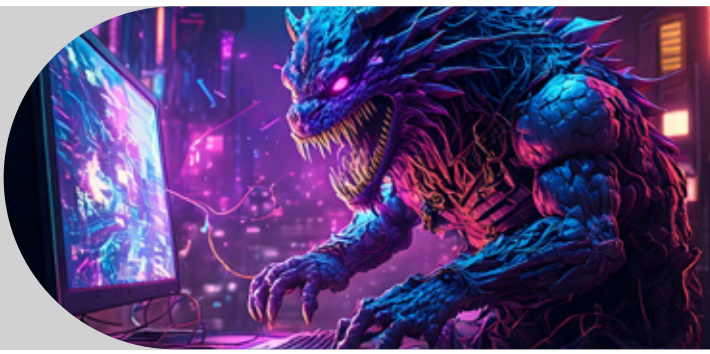
The FBI and CISA have issued a warning about the growing threat of the Medusa ransomware, a ransomware-as-a-service (RaaS) active since 2021. Since February alone, it has compromised over 300 victims. It primarily uses phishing campaigns to steal credentials and then applies double extortion tactics, encrypting data and threatening to leak it if the ransom is not paid.

Medusa runs a leak site where it lists victim names, countdown timers, ransom demands, and cryptocurrency wallet addresses for payment. It also allows victims to pay $10,000 to delay data exposure by one day.

Targeted sectors include healthcare, education, technology, and manufacturing. CISA recommends patching systems, enabling multi-factor authentication, and using strong passwords, although it advises against frequent password changes.

Exploitation of vulnerabilities in Ivanti

Ivanti issued a warning about two critical vulnerabilities (CVE-2025-0282 and CVE-2025-0283) affecting its Connect Secure, Policy Secure, and ZTA Gateway products. The first allows unauthenticated remote code execution, while the second enables local privilege escalation. Both vulnerabilities are currently being actively exploited.



GitHub Actions compromise

The recent GitHub Actions supply chain attack, which compromised over 23,000 repositories, has been linked to a previously undisclosed attack on March 11 targeting reviewdog/action-setup/v1 (CVE-2025-30154). This preceded the compromise of tj-actions/changed-files (CVE-2025-30066), which occurred between March 14–15 and led to secrets being leaked.

The attack began with a compromised personal access token tied to the @tj-actions-bot account, enabling the execution of a malicious Python script that extracted CI/CD secrets. At least 218 repositories were affected, leaking GitHub_Tokens.

The reviewdog incident was more limited in scope (1,500 repos over two hours) compared to the changed-files breach (14,000 repos over 22 hours). CISA added CVE-2025-30066 to its Known Exploited Vulnerabilities Catalog and urged organizations to review workflows run between March 14–15, revoke and rotate secrets, and implement strict access controls. GitHub also released guidance to help detect and prevent such attacks.

Attack on PyPI repository with JarkaStealer

Researchers discovered a campaign targeting the Python Package Index (PyPI), where malicious packages containing the JarkaStealer malware were uploaded. This malware was designed to exfiltrate sensitive information from infected systems.

maltiverse
Actionable Threat Intelligence

news

COMPROMISE OF THE POLISH SPACE AGENCY

Poland's Minister of Digital Affairs, Krzysztof Gawkowski, reported that the country's cybersecurity services detected unauthorized access to the IT infrastructure of the Polish Space Agency (POLSA). The attack was quickly contained, the compromised systems were secured, and investigations have begun to identify those responsible. As a precautionary measure, POLSA's network was disconnected from the internet to protect sensitive information while the scope of the incident is analyzed. The agency confirmed the cyberattack in statements to national media.

This incident occurs amid ongoing tensions between Poland and Russia, as Warsaw has repeatedly accused Moscow of attempting to destabilize the country due to its military support for Ukraine—claims that the Russian government denies. While the perpetrator has not been officially identified, the case has raised concerns about cybersecurity in Poland's critical infrastructure, particularly in strategic sectors like aerospace. Authorities are continuing their investigation to determine the origin of the attack and prevent future threats.

STORM-1865 PHISHING CAMPAIGN:PROJECT

The threat actor known as Storm-1865 has been carrying out a highly targeted phishing campaign against the hospitality sector, leveraging advanced social engineering techniques and tools like ClickFix to deliver various types of malware. Among the identified threats are XWorm, Lumma Stealer, and several remote access trojans (RATs), designed to take control of compromised systems or extract sensitive information.

These malicious campaigns are primarily aimed at credential theft and financial fraud. By infiltrating hotel systems and other organizations within the industry, the attackers seek access to banking data, payment systems, corporate emails, and other valuable resources. The sophistication of the techniques used, combined with the focused targeting of a sector particularly vulnerable to such attacks, has raised concerns among cybersecurity experts. They recommend strengthening defenses, training staff, and adopting proactive threat detection solutions to mitigate these risks.

ELON MUSK CLAIMS X WAS TARGETED IN A 'MASSIVE CYBERATTACK' DURING OUTAGE

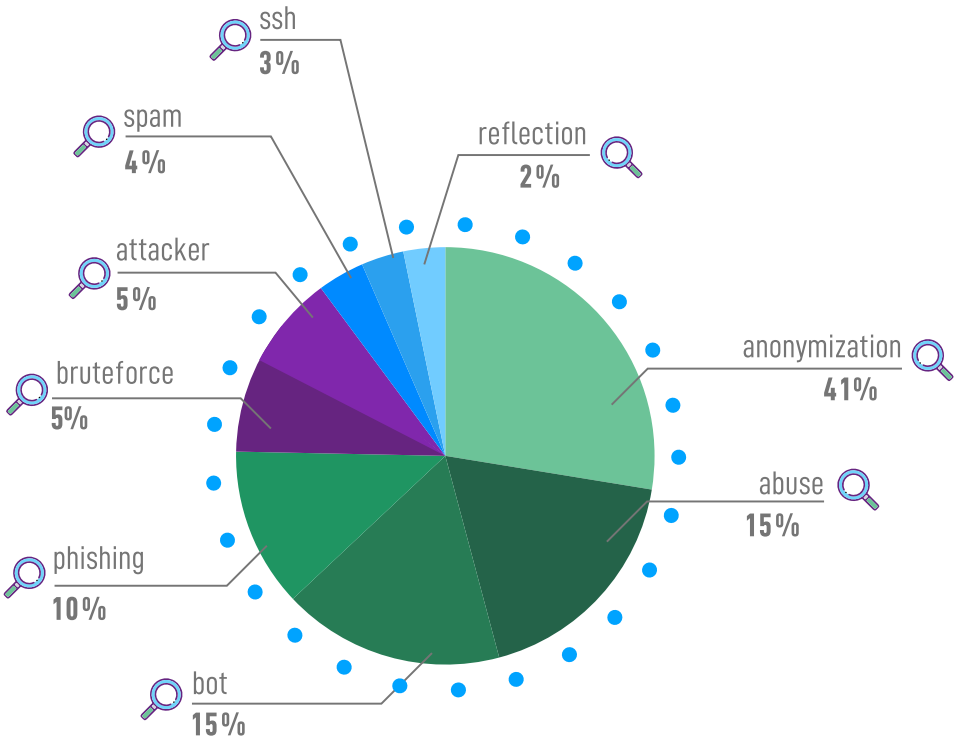
On Monday, March 10, 2025, the platform X (formerly Twitter) experienced several service outages affecting tens of thousands of users. Following the disruptions, Elon Musk claimed that X had been the target of a "massive cyberattack," suggesting that a coordinated group or even a nation-state might be involved, and mentioned that some IP addresses appeared to originate from the Ukraine region.

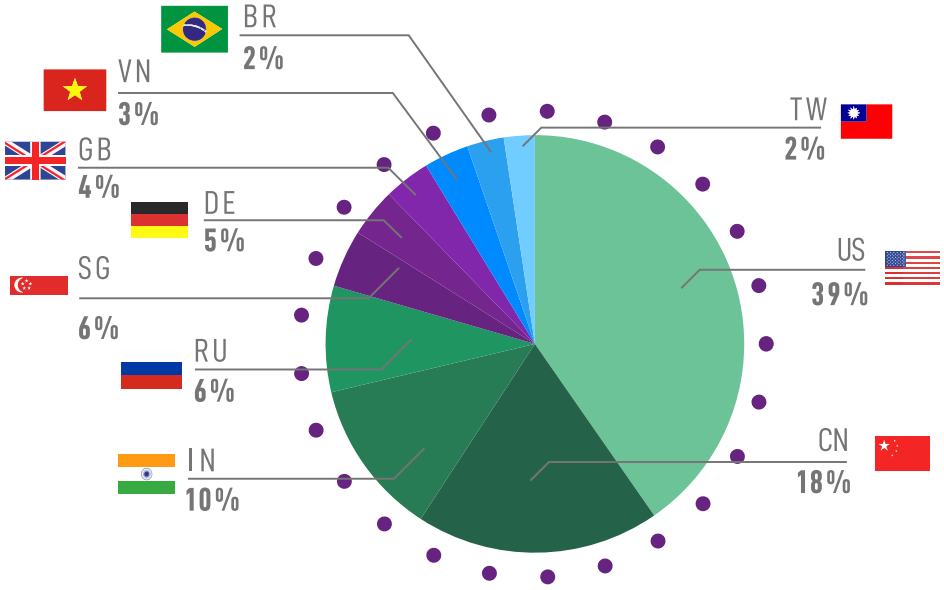
However, cybersecurity experts challenged this claim, stating the attack was part of a Mirai-based botnet made up of compromised cameras from around the world, not just Ukraine. Some researchers downplayed the incident, ruling out state actors and pointing out that such a short and visible attack would hold little value for a government. Although Musk did not provide technical data to support his version, the incident has reignited concerns about the security of X and how it is being managed under his leadership.

maltiverse
Actionable Threat Intelligence

REPORT

INDICATORS BY TYPE OF ACTIVITY



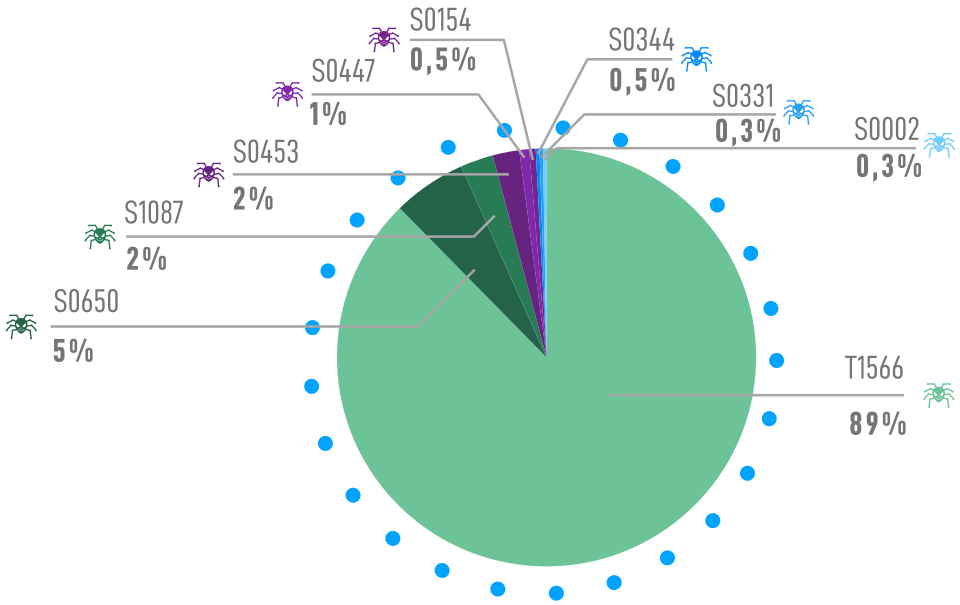


INDICATORS BY COUNTRY

maltiverse
Actionable Threat Intelligence

REPORT

MOST ACTIVE MALWARE FAMILIES



ID: T1566

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

PHISHING

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

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: S1087

Type: TOOL
Platforms: Windows
Version: 1.0

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

maltiverse
Actionable Threat Intelligence

REPORT

ID: S0453
Type: MALWARE
Platforms: Windows
Version: 1.0

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

ID: S0344
Type: MALWARE
Platforms: Windows
Version: 1.3

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

GROUPS THAT USE THIS SOFTWARE

G0092 - TA505

ID: S0331
Type: MALWARE
Platforms: Windows
Version: 1.3

AGENTE TESLA
Is a spyware Trojan written for the .NET framework that has been observed since at least.

GROUPS THAT USE THIS SOFTWARE

G0083 - G1018

ID: S0002
Type: TOOL
Platforms: Windows
Version: 1.9

MIMIKATZ
is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

GROUPS THAT USE THIS SOFTWARE

G0050 - G0016 - G1006 - G0046 - G0079 - G0092 - G1030 - G0060 - G0034 - G0064 - G1024 - G0131

LUMU ACQUIRES MALTIVERSE TO REDEFINE THREAT INTELLIGENCE, LAUNCHES EUROPEAN EXPANSION

Lumu, the cybersecurity company pioneering Continuous Compromise Assessment™, today announced its acquisition of **Maltiverse**, a Spain-based threat intelligence company specializing in curated threat feeds and malicious indicators of compromise (IOCs). This strategic acquisition enhances Lumu's ability to provide customers with deeper compromise context and strengthens its real-time threat intelligence capabilities.

"Cybersecurity is an intelligence-driven challenge, and the acquisition of Maltiverse allows Lumu to deliver even deeper threat visibility and response capabilities," said Ricardo Villadiego, Founder and CEO of Lumu. "By integrating Maltiverse's expertise in threat intelligence with Lumu's real-time compromise detection, we are not only enhancing our current offering, but we are also doubling down on our commitment to the market: helping organizations of all sizes and verticals operate cybersecurity proficiently."

Key Benefits of the Acquisition:

Enhanced Threat Actor Awareness – Lumu customers will gain deeper knowledge and understanding of how attackers operate, allowing them to proactively anticipate and defend against evolving and emerging cyber threats.

Expanded Compromise Context – Lumu customers will benefit from enhanced visibility into malicious activity, enriched by Maltiverse's deep and curated threat intelligence.

Stronger Cybersecurity Posture – The combination of Lumu's Continuous Compromise Assessment with Maltiverse's threat intelligence ensures organizations can proactively identify and mitigate threats before they escalate.

Strategic Geographical Expansion – This acquisition establishes Lumu's presence in the Iberian region as a foundational step toward expanding into the European market, positioning it for further growth in this strategic region.

"Joining Lumu marks an exciting new chapter for Maltiverse," said Hesaul Sanchez, CEO of Maltiverse. "Our mission has always been to provide high-fidelity threat intelligence to help organizations combat cyber threats effectively. By integrating our intelligence with Lumu's offerings, we are amplifying our impact, empowering more organizations with the knowledge and insights needed to stay ahead of cyber adversaries."

maltiverse
Actionable Threat Intelligence

PRODUCTS

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.

SOAR

SOAR technologies helps coordinate, execute and automate tasks between various people and tools all within a single platform. Maltiverse provides IoC context information and accurate classifications to create Playbooks and dramatically improve the quality of the decision making process.

FIREWALLS

At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. Maltiverse provides Threat Intelligence feeds that can be automatically synchronized with Firewalls to improve security for outbound connections to Command & Control servers or Malware distribution sites.

ROUTERS

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.

The Enteprise Plan offers a **30-day free trial for Enterprise customers**

Upgrade your **detection capabilities**

START 30 days TRIAL

Actionnable threat INTELLIGENCE

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 30 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 30 days TRIAL