CYBERINT WEEKLY >REPORT

A Threat Actor Claims to Have RCE Exploit in Albatross Protocol

A threat actor offers a remote code execution (RCE) exploit for the Albatross Protocol, exploiting a buffer overflow vulnerability. However, the exploit has limitations with certain security measures.

EXCLUSIVE
RCE
EXPLOIT

Data Breach Exposes Sensitive Information of Care Vision Users

In July 2024, the threat actor Hana posted details of a data breach on Breachforums, affecting Care Vision, a UK-based cloud Care Management system.

BREACH
CARE VISION
UK

RansomHub Group Allegedly attacked Garudafood Putra Putri Jaya

The RansomHub ransomware group has allegedly attacked Garudafood Putra Putri Jaya, a company in the Food & Beverages sector in Indonesia. The group claims to have obtained 10G of data and threatens to publish it within one day.

RANSOMWARE
RANSOMHUB
INDONESIA

'Zeus' Leaks Personal Information of Israeli Olympic Delegation Members

A new threat actor known as 'Zeus' has published personal information about the members of the Israeli 2024 Olympic delegation. The exposed data includes phone numbers, email addresses, home addresses, ID numbers, family relations, etc.

ZEUS
LEAKS
OLYMPIC

Administrator Access to Israeli Agricultural-Chemical Company Offered for Sale

A threat actor known as "ZeroSevenGroup" has listed administrator access to an Israeli agriculture company for sale on a cybercrime forum, priced at 2000 USD.

ISRAEL
ZEROSEVEN GROUP
AGRICULTURAL

Threat Actor offering for sale over 14.5 Million lines of Chilean Citizens Data

The threat actor ViralGod is offering for sale on the cybercrime forum "breach forums" a database of Chilean Citizens. The threat actor claims to have over 14.5 million lines of citizens' information, including RUT (Tax ID), Full name, address, Region, and Comuna.

SALE
VIRALGOD
CHILE

RA World Ransomware Group Has Allegedly Attacked Melchers Singapore

RA World Ransomware Group has added four new victims to their dark web portal, including The Singapore Branch of Melchers Group. They're threatening to publish the data they acquired during the attack in a week (01/08)

RANSOMWARE
SINGAPORE
RA WORLD

Threat Actor shared a file that includes 49 SQL Databases from multiple Mexican websites

The Threat Actor ViralGod posted on the cybercrime forum " Breachforums," a file that claims to contain 49 SQL databases from different Mexican websites. The threat actor claims to have over 1,000,000 lines, most containing users' information, such as emails, full names, addresses, and phone numbers.

VIRALGOD
BREACHFORUMS
LEAK

Group of Cyber Criminals conducting Vishing Attacks Local Philippine Banks Arrested

A group of Vishing operators - composed of 9 members - was arrested by Philippine local police on July 25, 2024. These operators mainly target local bank customers, especially the elders (Senior Citizens).

VISHING
ARREST
PHILIPPINES

Threat Actors are abusing Google Cloud to Harvest Credentials via Phishing

The Threat Actor FLUXROOT has been seen targeting LATAM users. It aims to harvest login information associated with different online payment platforms in the LATAM region by leveraging Google Cloud serverless projects.

CLOUD
FLUXROOT
LATAM

NEW WEEKLY VULNERABILITIES

CVE-2024-6327

TELERIK CVSS: 9.9

Telerik Report Server is a web-based application for creating, managing, and delivering reports in various formats, featuring tools for report design, scheduling, and secure delivery to centralize reporting processes. The issue at hand stems from insecure deserialization, where untrusted data is deserialized, potentially allowing attackers to execute arbitrary code remotely on the affected server. Progress has not disclosed whether CVE-2024-6327 has been exploited in the wild.

CVE-2024-41110

DOCKER CVSS: 10.0

Docker has identified a critical flaw in specific versions of Docker Engine, potentially allowing attackers to bypass authorization plugins (AuthZ) under certain conditions. This vulnerability, tracked as CVE-2024-41110 has a CVSS score of 10.0, indicating extreme severity. An attacker could exploit this flaw using an API request with Content-Length set to 0, causing the Docker daemon to forward the request without the body to the AuthZ plugin, which might incorrectly approve it. Exploiting Docker Desktop requires access to the Docker API, implying that the attacker must have local access to the host machine unless the Docker daemon is insecurely exposed over TCP.

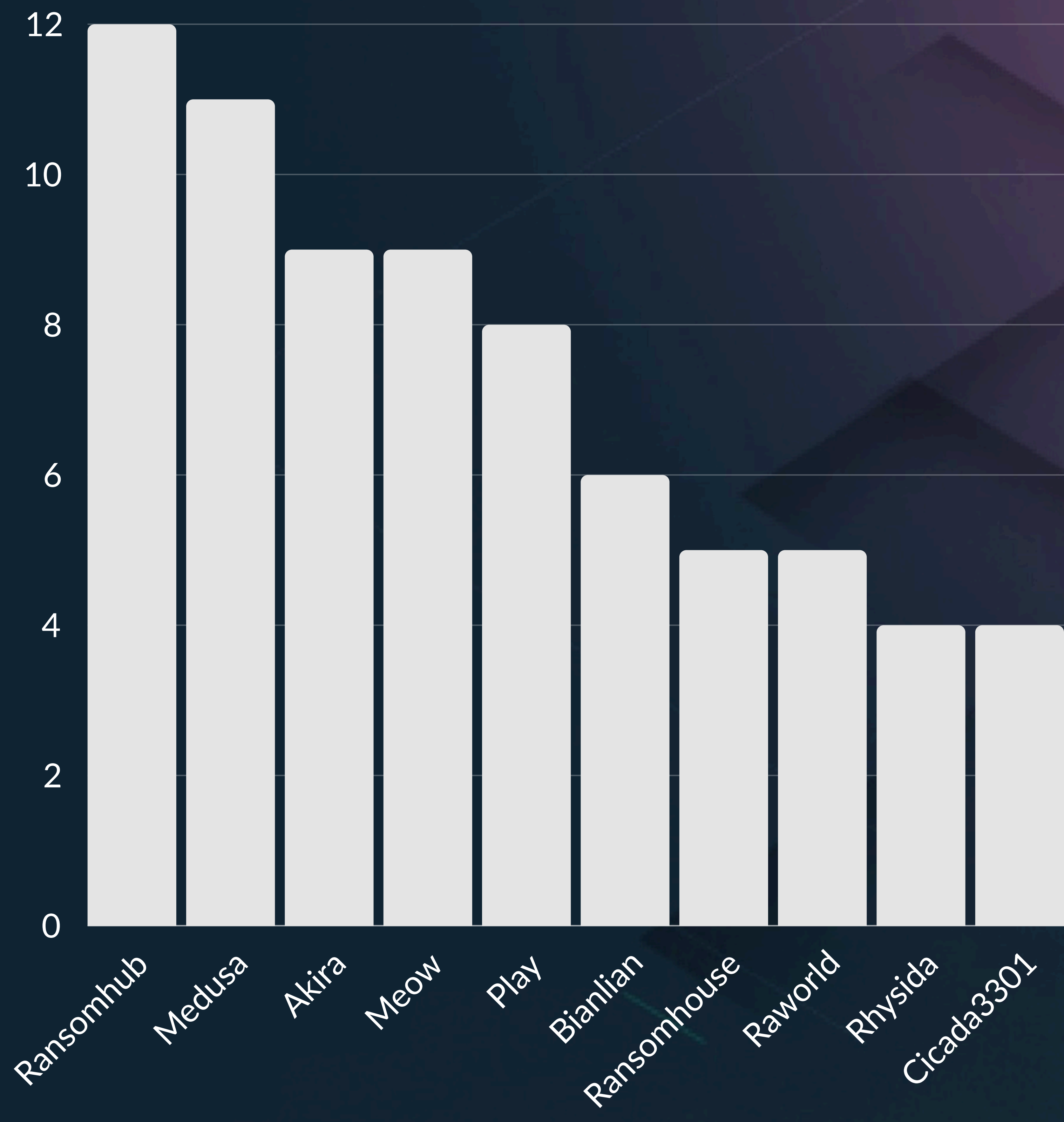
CVE-2024-0760

ISC CVSS: 7.5

The Internet Systems Consortium (ISC) has released security advisories to address vulnerabilities in multiple versions of ISC's Berkeley Internet Name Domain (BIND) 9, including CVE-2024-0760. A cyber threat actor could exploit one of these vulnerabilities to cause a denial-of-service condition. A malicious client can send numerous DNS messages over TCP, potentially destabilizing the server during the attack. The server may recover after the attack ceases, but using ACLs will not mitigate the attack. The server can remain unresponsive for some time after the attack ends. This flaw was discovered during internal testing, and there are no known active exploits.

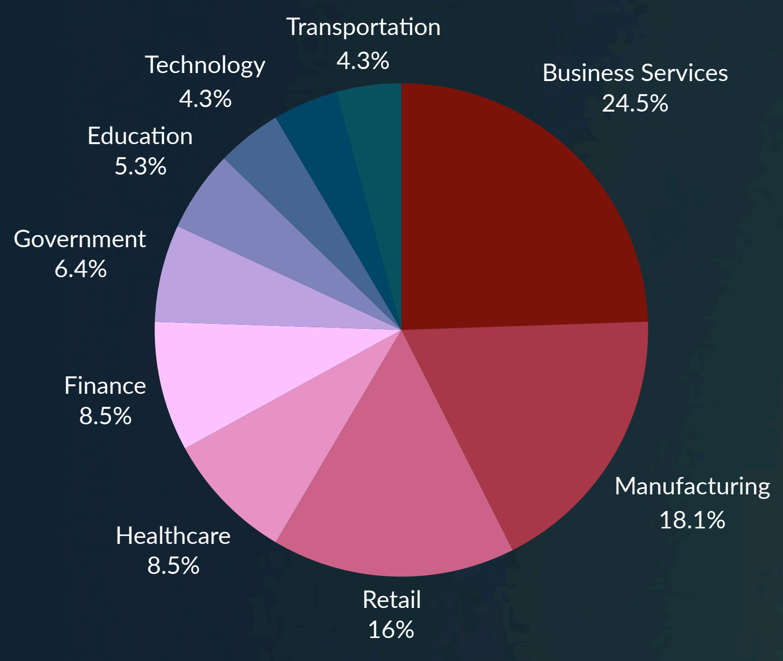
WEEKLY RANSOMWARE STATS

WEEKLY TOP RANSOMWARE FAMILIES

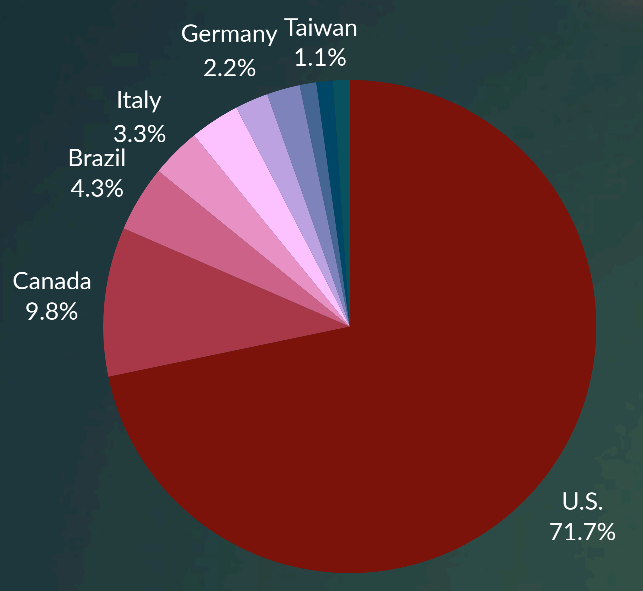


- RANSOMHUB LEADS THE RANSOMWARE INDUSTRY THIS WEEK WITH 12 NEW VICTIMS
- IN SECOND PLACE, MEDUSA COMPROMISED 11 NEW VICTIMS THIS WEEK
- AKIRA IS IN THIRD PLACE WITH NINE NEW VICTIMS THIS WEEK

TOP TARGETED SECTORS DISTRIBUTION



TOP TARGETED COUNTRIES DISTRIBUTION


Germany
Taiwan
Italy
Brazil
Canada
U.S.