2024

THE STATE OF THE INTERNET

THE OPENCANARY EXPERIENCE

April 2025

Lee Mössner

www.toce.ch

Table Of Contents

Executive Summary

Throughout 2024, three OpenCanary honeypots operated with open ports exposed to the Internet. These ports were **scanned and tested** approximately **2,500 times per hour**, offering a clear view of what threat actors are actively searching for online.

The results are striking: the honeypots recorded over **69 million access attempts**, with the attacks appearing to fall into **three distinct categories**.

Take Control

Nearly **49 million** attempts targeted the honeypots with the goal of **seizing control** of the machines and their resources.

Steal Data

More than **19 million** attempts focused on **gaining direct access to database protocols**, aiming to exfiltrate stored information.

Access File Systems

1.5 million attempts were made to try to access the host filesystem with thousands of files dropped onto the hosts in an attempt to infect them.

The Honeypots

Three honeypots, powered by OpenCanary from Thinkst, are deployed across three distinct locations, each with identical ports and protocols exposed to the Internet.

These devices sit and listen for connection requests on a variety of TCP ports and log what they find.

No login or connection attempt will ever be successful.

Thing 1, Thing 2 and Thing 3 - OpenCanary honeypots

Hacker Motives

The vast amount of logging data makes one thing clear: any Internet-facing host, regardless of how well-patched it is, will come under attack. These attacks are cheap to execute but can yield significant rewards, as countless vulnerable hosts are continuously discovered, compromised, and recruited into botnets.

Ransomware and extortion are also key objectives for threat actors, who encrypt or steal data to pressure victims into paying a ransom—typically in Bitcoin or other digital currencies—to regain access or prevent data leaks.

Taxonomies

The attack patterns fall into two main categories: to take control of the host or to steal data from the host. Attackers probe the honeypots' ports either to gain control of the host itself or to access the data it stores and serves.

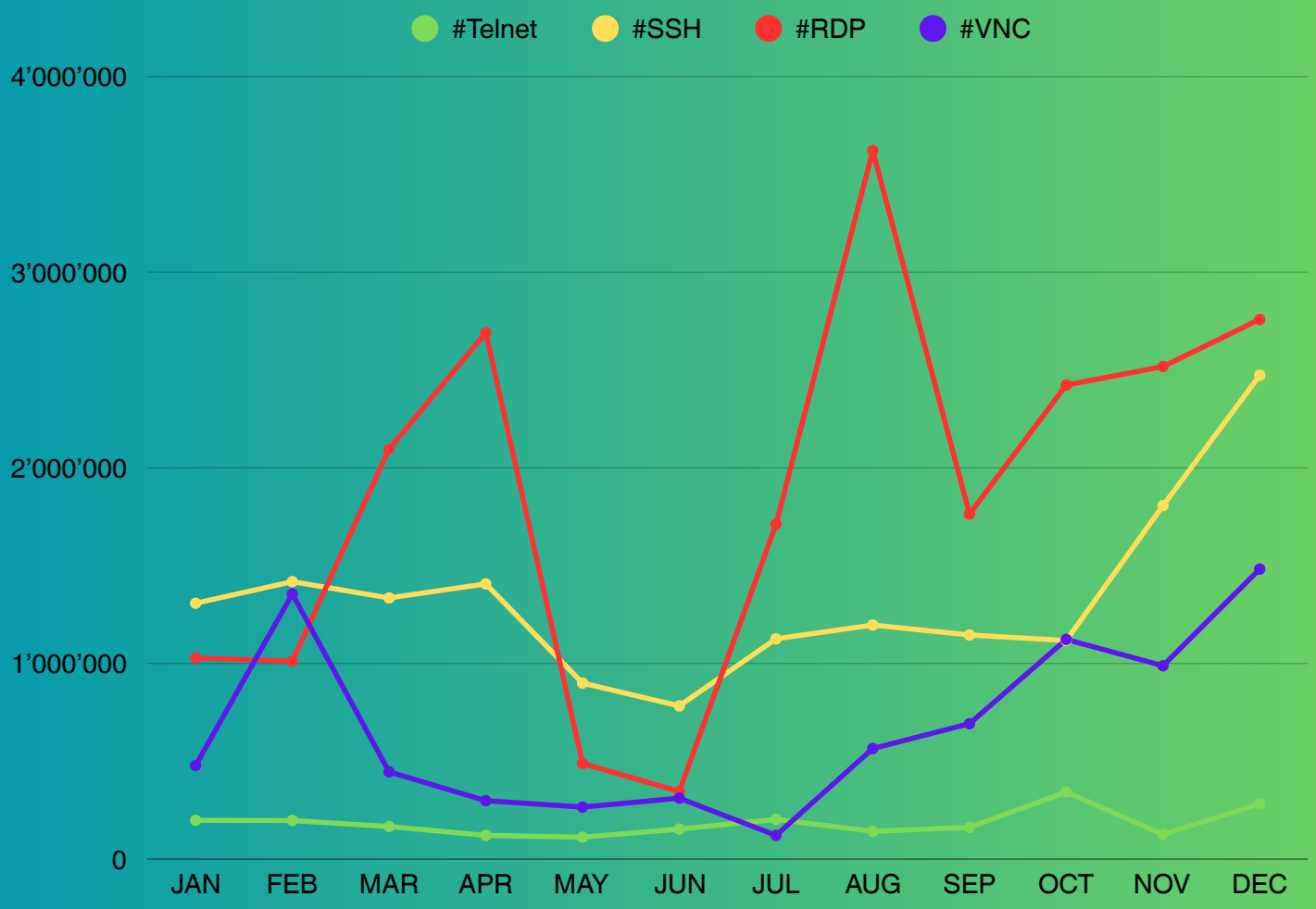
- ## Take Control

  These attacks target both command-line protocols (22/SSH, 23/FTP) and graphical protocols (3389/RDP, 5901/VNC), with the goal of gaining privileged access to the host and establishing a persistent foothold.

- ## Steal Data

  Attacks aiming to access data fall into two categories: file-level and database-level intrusion. File-level attempts focus on FTP and SMB services (ports 21 and 445), while database-level attacks target MySQL, MSSQL, and REDIS services (ports 3306, 1433, and 6379).

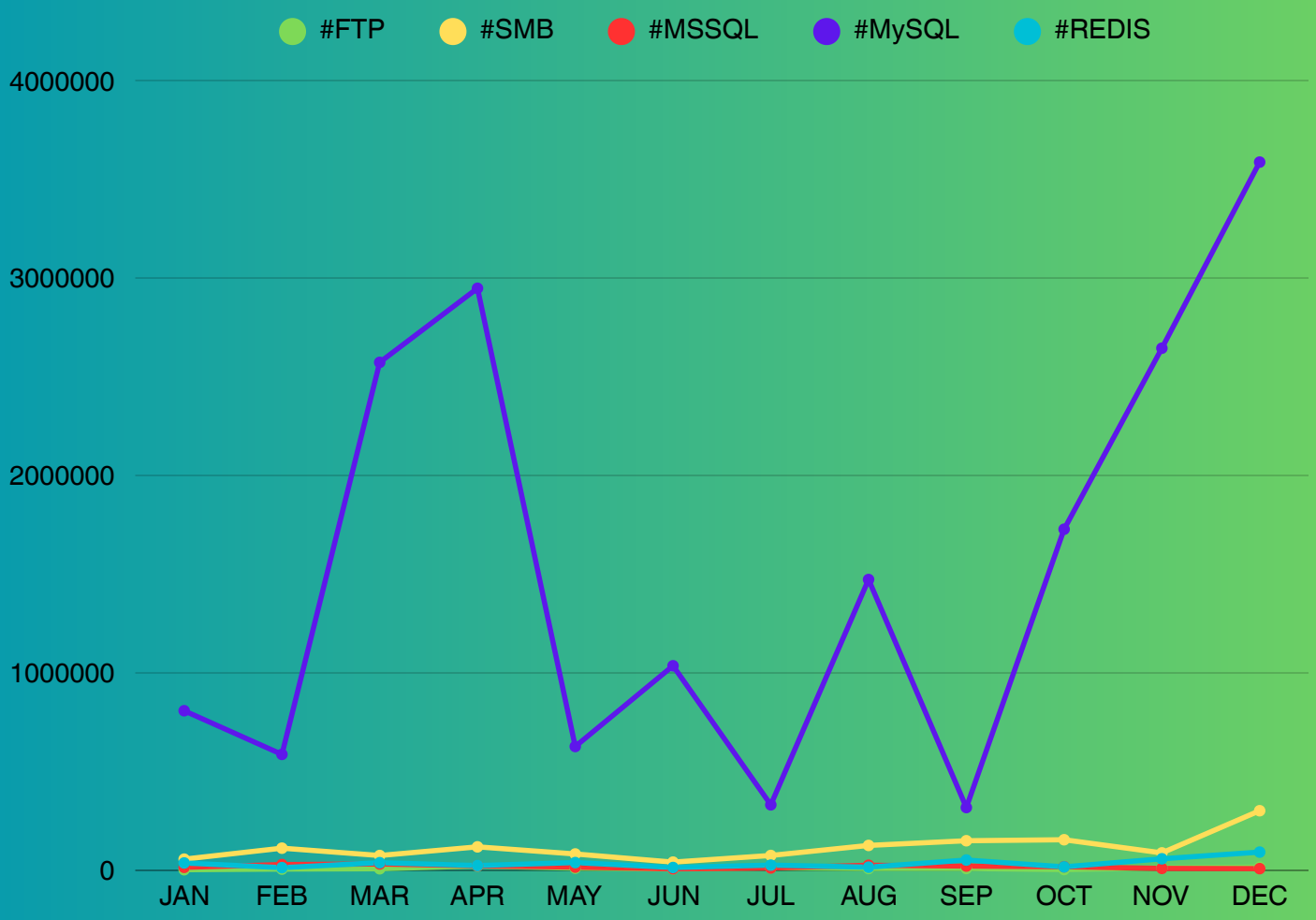
Take Control



While the deprecated clear-text protocol Telnet continues to appear in attack traffic, its presence remains consistently low. In stark contrast, significantly higher volumes of attempts are directed at more modern and potentially rewarding services like SSH, VNC, and RDP — all of which offer attackers the possibility of privileged, interactive access if compromised.

These relentless scans and attacks are simply part of life on the Internet. Anyone deploying hosts on the global network must understand that exposing these ports and protocols is a critical mistake. Instead, VPNs and key-based or other non-password authentication methods should be employed to minimize the attack surface and protect these services from constant probing.

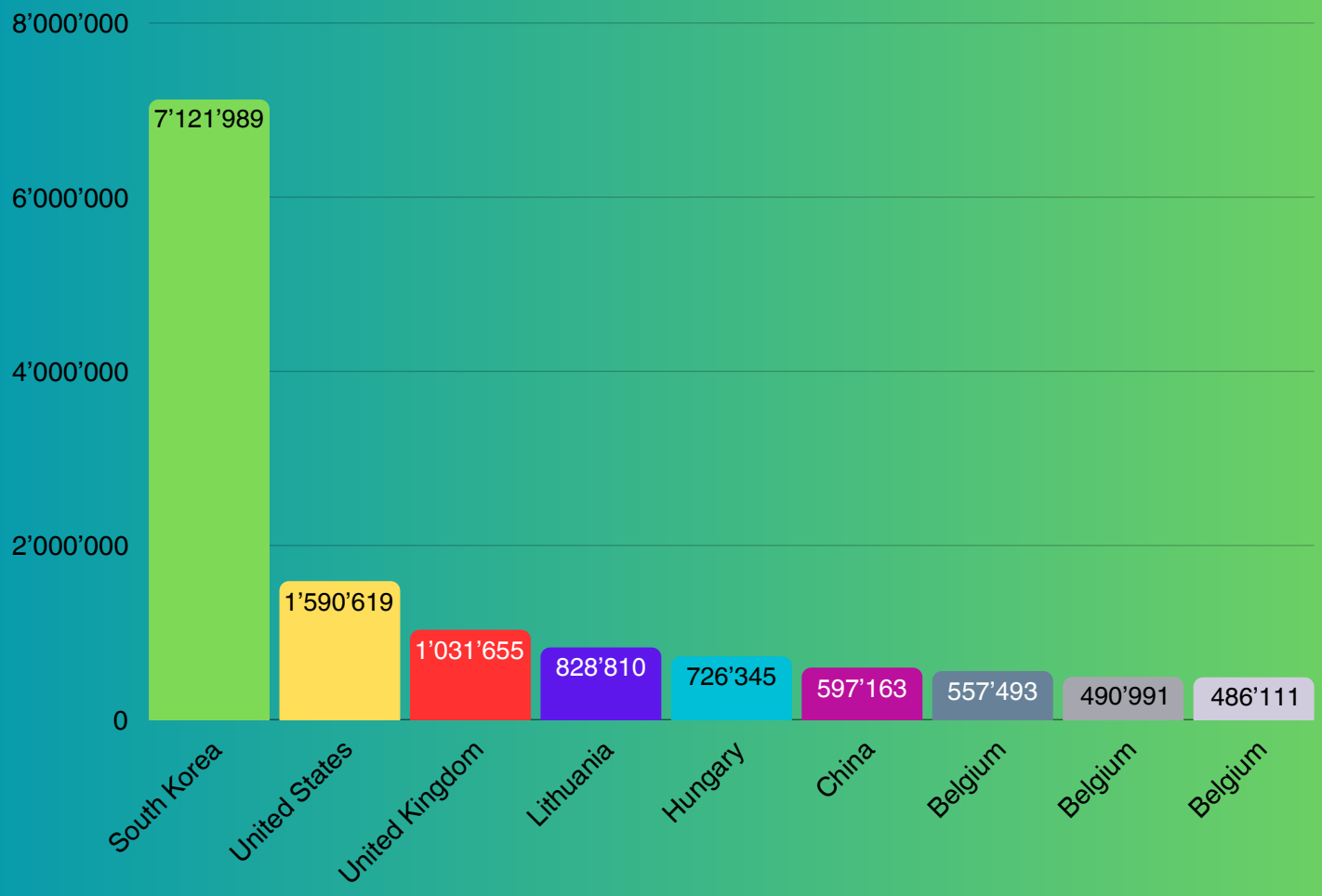
Steal Data



MySQL (and its variant, MariaDB) stands out as the primary target for attackers seeking data access. The volume of attempts against this service far exceeds the combined attack traffic seen on FTP, SMB, MSSQL, and Redis, underscoring its attractiveness to threat actors.

Unlike in the Host Compromise category, Microsoft protocols are far less targeted in the realm of Data Compromise. This disparity is largely due to the widespread use and popularity of MySQL and its fork, MariaDB, which dominate attacker interest in data access attempts.

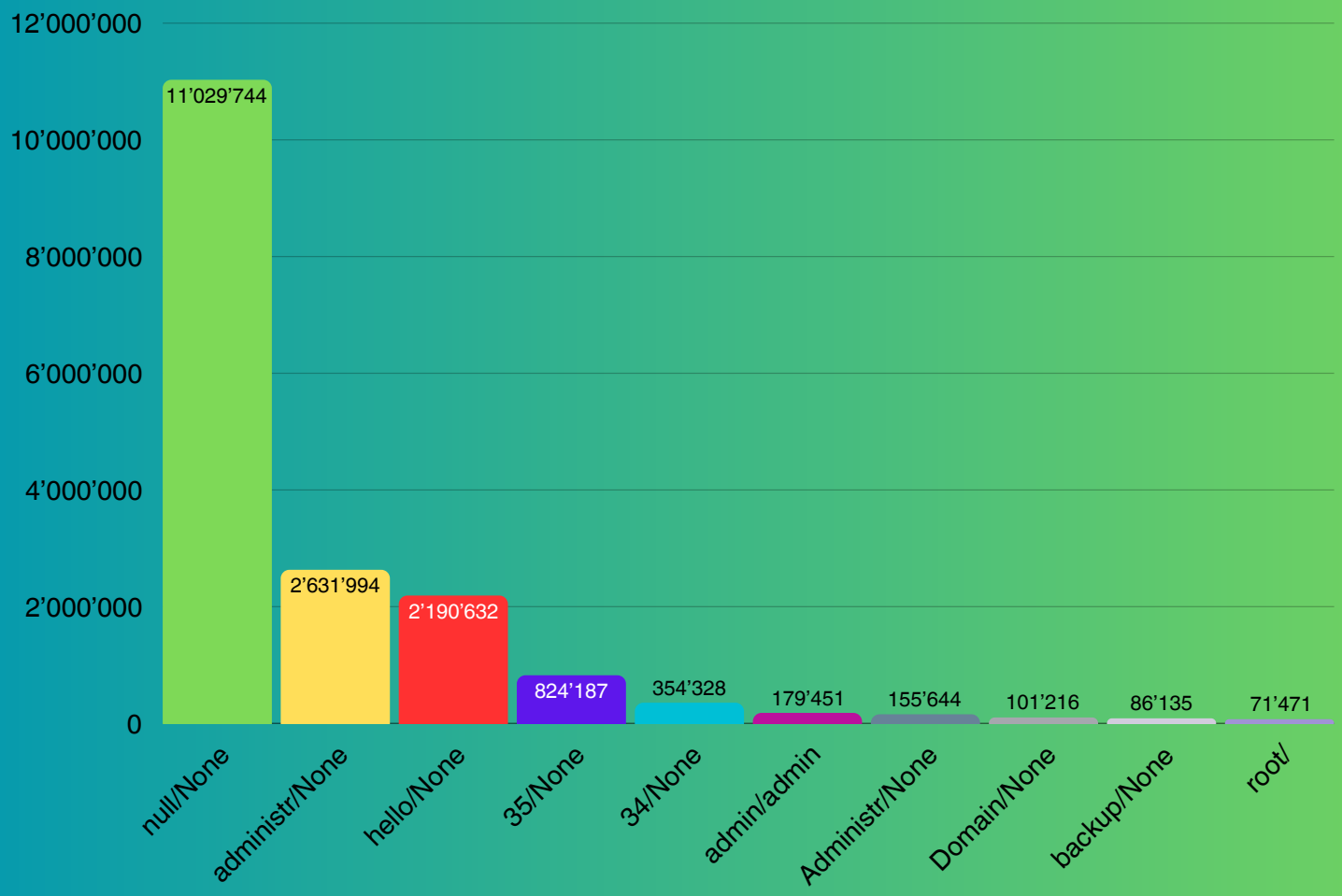
Attack Sources



A South Korean IP address was responsible for the highest volume of attack traffic, generating four times more activity than the next leading source.

Unlike in the Host Compromise category, Microsoft protocols are far less targeted in the realm of Data Compromise. This disparity is largely due to the widespread use and popularity of MySQL and its fork, MariaDB, which dominate attacker interest in data access attempts.

Weak Credentials

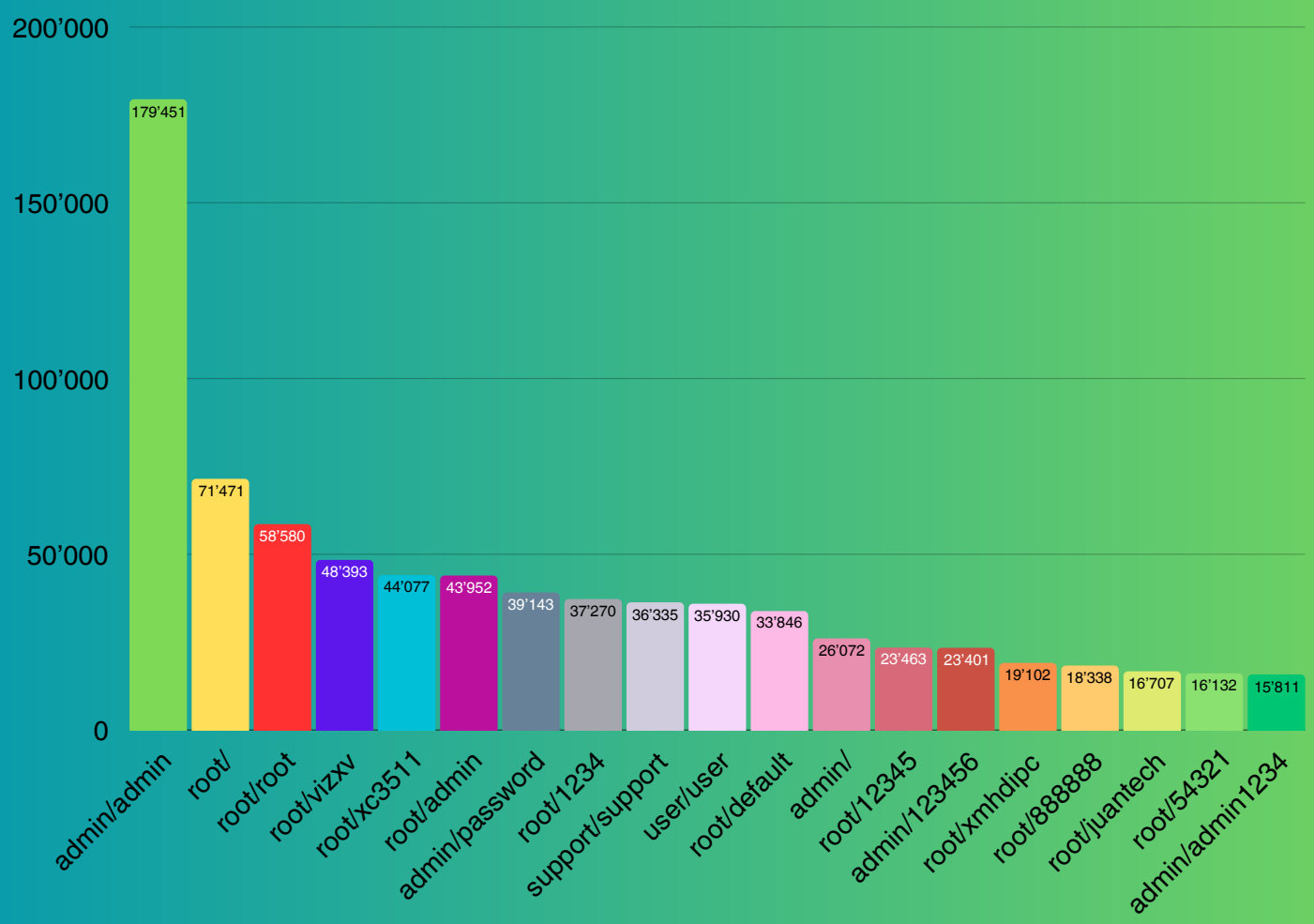


The most commonly attempted credentials likely reflect the way attack scripts are designed, which, in turn, may indicate the skill level and approach of the threat actor deploying them.

The top 50 credentials captured by the honeypots accounted for over 18 million login attempts on Telnet and SSH ports in 2024, out of a total of more than 24 million attempts.

Attackers attempted to gain access to the exposed hosts using thousands of different credentials.

Is that you, Mirai?



Nineteen of the top 50 credentials used in login attempts against OpenCanary honeypots are directly linked to the Mirai botnet. These credentials accounted for 1.6 million login attempts, making up approximately 9% of the total attempts using the top 50 credentials in 2024.

The Mirai botnet was first discovered and named in 2016. While the botnet itself may no longer be active, its foundation—exploiting the 60 default credentials found on Internet-connected devices—remains a significant security risk. A substantial volume of automated traffic continues to scan for vulnerable devices, attempting to recruit them into similar botnets.

Summary and Conclusion

Internet hosts aren't only at risk due to unpatched vulnerabilities—poor configurations, including default settings or outright reckless setups, significantly increase the likelihood of compromise.

Attackers seek to establish a foothold on any machine they can compromise, using it as a launchpad to pivot deeper into the network, steal data, disrupt operations, or further their own campaigns. Ultimately, their goal is financial gain—ideally, a quick and lucrative payday.

One unexpected outcome of running a honeypot with open file shares was that threat actors actively deposited files, hoping they would be executed. A total of 24,159 files were dropped onto the honeypots, with the most common being a Windows RAT designed to launch a remote shell.

It should be evident to anyone deploying hosts and services on the Internet that this process requires careful planning and consideration. Reducing the attack surface is crucial, and with the right precautions in place, automated hacking attempts—whether targeting the host or its data—can be effectively mitigated.

This report contains a high-level summary of the data. The full dataset, containing 69 million entries, provides far deeper insights—revealing which attacks originate from specific IP addresses, the millions of usernames and passwords used in attacks, and much more. Use the contact details below to find out more.

Contact

internet2024@toce.ch

www.toce.ch