2024

Global Threat Year-in-Review

EXECUTIVE SUMMARY

From the exploitation of large language models (LLMs) to the increased use of automation, growing scale of attacks, and weaponization of open source tools, the 2024 Sysdig Threat Report delves into the expanding attack surface and financial strain that cloud-based organizations face.

Some attacks, such as ransomware, deliver high-impact financial blows, while others are more subtle, siphoning resources over time. Drawing from novel threats reported by the Sysdig Threat Research Team (TRT), the report highlights trends underscoring the need for real-time threat detection and rapid response.

PLAYING THE ODDS

The newest AI drain on cloud resources

First identified by the Sysdig TRT in May 2024, LLMjacking — the theft of cloud accounts to exploit large language models — can cost victims more than $100,000 in daily resource consumption charges. Mirroring earlier cryptojacking and proxyjacking techniques, LLMJacking marks a significant and costly evolution in resource-jacking.

TURNING THE TABLES

Using good tools for evil

Sysdig TRT observed the weaponization of multiple open source tools this year, notably SSH-Snake, which facilitated credential theft and expanded attacks across the US, China, and beyond. Less than a month after the tool's release, the CRYSTALRAY threat group leveraged the newly created pen testing tool to steal more than 1,500 victims' credentials.

THE LONG GAME

Stealth and persistence

DDoS attacks are often overlooked because their impacts are underestimated and they're typically considered to be easy to detect and remediate. While RebirthLtd, a DDoS-as-a-Service botnet, is marketed for video game servers, it poses risks of data exfiltration and espionage if misused. On the other hand, RUBYCARP, a stealthier botnet group, prioritized defense evasion and remained undetected for over a decade before Sysdig TRT's discovery.

RISKY BETS

Gambling on market trends

Forward-thinking and financially motivated attackers, with eyes on market trends and cryptocurrency projections, were found exploiting legitimate tools and stolen account access to mine Meson Network (MSN) crypto prior to its token unlock a few months later. These attackers made a risky bet; if the worth of MSN went up, the mining campaign would be a jackpot.

sysdig

COPYRIGHT © 2024 SYSDIG, INC. ALL RIGHTS RESERVED.
EXEC-SUM-RP003 REV. A 10/24

READ THE FULL REPORT →