REDISRAIDER: A STEALTHY CRYPTOJACKING CAMPAIGN TARGETING UNSECURED REDIS SERVERS

Vairav Cyber Security News Report

Date: May 09, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Datadog Security Research has uncovered a sophisticated Linux-based cryptojacking campaign named **RedisRaider**, which targets publicly exposed **Redis servers**. The campaign demonstrates strong operational maturity, employing Go-based payloads obfuscated with Garble, runtime unpacking of the miner, and subtle anti-forensics tactics such as short key time-to-live (TTL) and database manipulation. Using compiled Go binaries, complex unpacking routines, and obfuscated infrastructure shows that RedisRaider is not a typical opportunistic cryptojacking campaign. Instead, it reflects a highly engineered, scalable operation targeting misconfigured cloud workloads.

KEY FINDINGS

- RedisRaider is a new cryptojacking campaign that secretly uses the computing power of Linux systems running Redis to mine cryptocurrency (Monero) for financial gain.
- The attackers focus on unsecured Redis servers that are exposed to the internet without proper protection.
- The campaign is well-planned and technically advanced, using hidden scripts and tools to avoid detection and leave minimal traces behind.
- The main malware is disguised as a regular image file and quietly runs in the background.
- RedisRaider's creators also run a browser-based mining operation, which can mine cryptocurrency directly through a user's web browser if they visit an infected website.
- The campaign uses infrastructure hosted in South Korea, with payloads and mining tools stored on multiple suspicious domains.

THREAT OVERVIEW

- **Malware:** RedisRaider (Go-based dropper)
- **Delivery Method:** Injected via Redis misconfiguration using legitimate Redis commands (SET, CONFIG, BGSAVE) to place malicious cron jobs
- **Initial Lure:** No external lure used, exploitation is automated and targets publicly exposed Redis servers.

- **Attack Vector:** Internet-facing Redis instances with no authentication or running in unprotected mode.
- **Payload Obfuscation:** Obfuscated using Garble (Go obfuscation tool), custom packers, in-memory unpacking, and misleading file names (e.g., disguised as a .png image).
- **Target Platform:** Linux systems running Redis, specifically x86-64 architecture.

INCIDENT ANALYSIS

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) – REDISRAIDER CAMPAIGN

Initial Access

- Scans the randomized IPv4 address space for publicly exposed Redis servers on port 6379.
- Issues the Redis INFO command to confirm the target is running on Linux.
- Exploits Redis misconfigurations by injecting malicious cron jobs using SET and CONFIG commands.
- Attempts to authenticate with hardcoded credentials if authentication is enabled.

Execution

- Delivers a base64-encoded shell script via Redis cron injection to download the main payload from a hardcoded URL.
- Drops the RedisRaider binary as /tmp/mysql, grants it execution permissions, and runs it via nohup for background execution.

Persistence

- Redis dumps a fake cron job file to /etc/cron.d/apache using modified CONFIG parameters (dir, dbfilename, bgsave).
- Spawns multiple Goroutines for concurrent scanning, exploitation, and miner deployment.
- Continues scanning loop for new Redis targets and propagates autonomously.

Payload Activity

- The main payload is a Go-based ELF binary that drops a packed XMRig miner.

- Conducts hardware profiling (CPU cores, huge page size, ulimit) to optimize mining performance.
- Uses in-memory unpacking and runtime execution of the miner.

Command and Control (C2)

- Tests connectivity using httpbin[.]org before beginning scanning.
- Primary payload and miner are hosted at http://a.hbweb[.]icu:8080/....

Defense Evasion

- Payloads obfuscated with Garble, a Go compile-time obfuscator.
- Strips debug symbols and embeds miner in non-executable sections.
- Uses custom unpacking logic with runtime decryption.
- Employs short TTLs, deletes Redis keys (del t) post-injection, and uses misleading file extensions (e.g., .png).

Monetization Strategy

- In addition to system-level mining, the actor hosted a browser-based Monero miner on c[.]hbweb[.]icu, indicating a multi-vector cryptojacking campaign.
- Web miner was configured to use the MoneroOcean pool with the wallet: *41nTqsXxuM8bPENEBDf1YmH9yKBhpfsJbgQGEcVetSsk2qCE5J97xtCAiDb7CQva8u7i9735rragqeiT2rN9Ekb91sMZ92G.*

Conclusion

RedisRaider is a sophisticated Linux cryptojacking campaign that targets exposed Redis servers, using a custom XMRig miner, stealth techniques, and worm-like spread. It also leverages in-browser mining for broader monetization. This highlights the urgent need to secure public-facing services with strong authentication and active monitoring, as cryptojacking threats are now highly targeted and well-executed.

INDICATORS OF COMPROMISE (IOCs)

IP Address

58[.]229.206[.]107

Malicious URLs

http://a.hbweb[.]icu:8080/uploads/2024-7/99636-5b0c-4999-b.png

File Hashes

8d2efe92846cdf9c258f0f7e0a571a8d63c80f0fa321cb2c713fb528ed29ba42

7b2314bf8bf26ce3f3458b0d96921d259ee7b0be1c0b982c2a19d8c435b7e3ae

RECOMMENDED ACTIONS

- **Secure Redis Deployments:** Ensure Redis servers are not exposed to the public internet. Enable authentication and run Redis in **protected mode** by default.
- **Use Firewalls and Network Segmentation:** Limit access to Redis instances using **firewall rules**, **security groups**, or **private network configurations**.
- **Monitor Cron Jobs and File Changes:** Regularly audit /etc/cron.d/ and system directories for unauthorized entries or unexpected scripts.
- **Scan for Known IOCs:** Continuously scan environments for indicators of compromise (IOCs) such as unusual file paths, suspicious binaries, or known malicious domains/IPs.
- **Deploy Behavior-Based Detection Tools:** Use runtime protection (e.g., eBPF-based agents) to detect unexpected execution patterns like hidden miners or system resource misuse.
- **Keep Systems Updated:** Apply patches regularly and stay current with Redis and system-level security updates.
- **Educate DevOps Teams:** Raise awareness about the risks of misconfigured services and the importance of secure-by-default deployments in production environments.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com