15 July 2026

TLP: WHITE

INTEL471

# EMERGING THREATS

## QuimaRAT

QuimaRAT is a newly identified Java-based Remote Access Trojan (RAT) that is being marketed under a Malware-as-a-Service (MaaS) model, and providing threat actors with a cross-platform remote access framework capable of targeting Windows, Linux, and macOS systems. As opposed to many traditional RATs that focus on a single operating system, QuimaRAT was designed from the outset to support multiple platforms through a modular architecture that allows operators to dynamically expand functionality using encrypted plugins delivered from its command and control infrastructure. Researchers observed that the malware suite includes not only the RAT itself, but also a dedicated builder, loader, and dropper capable of generating numerous payload formats to support a wide variety of delivery methods. It is worthy to note that QuimaRAT lowers the barrier to entry for cybercriminals by offering subscription-based access, allowing less sophisticated operators to leverage advanced remote access capabilities without developing their own malware.

# QUIMARAT HUNT COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('9cc597ba-a530-4215-a8a0-8408bc00f292'),touched:!t)

# RELATED HUNT PACKAGES

## Autorun or ASEP Registry Key Modification

https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

## CronJobs Pointed at Hidden Directories - Linux

https://hunter.cyborgsecurity.io/research/hunt-package/c9b77333-a233-4e86-8cba-9675686375df

## Hiding Files And Directories

https://hunter.cyborgsecurity.io/research/hunt-package/e4180bd5-f5ed-47ac-8df4-f88ce6a371c7

## File Created In Startup Folder

https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee

## PLIST File Created in Common Launch at Boot Folders in MacOS - Potential Persistence

https://hunter.cyborgsecurity.io/research/hunt-package/6345f730-3b8a-4e7a-8a6f-a68aff660ad8

## Potential Use of Findstr or Find with Tasklist

https://hunter.cyborgsecurity.io/research/hunt-package/ee9bb6c4-378e-498e-ad04-fe469da49046

### macOS Persistence - LaunchAgents

https://hunter.cyborgsecurity.io/research/hunt-package/afe15290-19a1-4891-b8a0-0f0f64c67961

### Scheduled Task Deleted - Possible Hiding Tracks Behavior

https://hunter.cyborgsecurity.io/research/hunt-package/391065c9-40f9-48fa-a033-9a28fbd66dc1

# THREAT SUMMARY

QuimaRAT is a newly identified Java-based Remote Access Trojan (RAT) that is being marketed under a Malware-as-a-Service (MaaS) model, and providing threat actors with a cross-platform remote access framework capable of targeting Windows, Linux, and macOS systems. As opposed to many traditional RATs that focus on a single operating system, QuimaRAT was designed from the outset to support multiple platforms through a modular architecture that allows operators to dynamically expand functionality using encrypted plugins delivered from its command and control infrastructure. Researchers observed that the malware suite includes not only the RAT itself, but also a dedicated builder, loader, and dropper capable of generating numerous payload formats to support a wide variety of delivery methods. It is worthy to note that QuimaRAT lowers the barrier to entry for cybercriminals by offering subscription-based access, allowing less sophisticated operators to leverage advanced remote access capabilities without developing their own malware.

Over the past several months, QuimaRAT has evolved into a comprehensive malware platform rather than a standalone remote access trojan. Reporting indicates that the malware is capable of targeting organizations globally, particularly those operating Windows, Linux, and macOS environments where cross-platform administration is common. The framework enables malicious actors to establish persistent remote access, execute arbitrary commands, deploy additional payloads, steal credentials, monitor user activity, and exfiltrate sensitive information from compromised systems. The combination of modular plugin support, multiple delivery mechanisms, and operating system specific persistence techniques makes QuimaRAT a highly flexible threat capable of adapting to diverse enterprise environments. Given its continued development and commercial availability, it is important to assess, understand, and prepare for this threat as adoption among cybercriminals continues to increase.

# THREAT SYNOPSIS

At the outset, QuimaRAT has been observed utilizing a dedicated builder and loader framework capable of producing payloads in numerous formats including JAR, EXE, APP, SH, BAT, and VBS, allowing operators to tailor delivery methods for specific victim environments. Researchers also observed dedicated loader and dropper components that leverage browser cache delivery techniques using lures such as fake CAPTCHA pages and software update prompts to stage payloads while reducing the likelihood of detection. Once executed, the malware determines the host operating system before enabling operating system specific functionality, performs environment validation, and creates a lock file to ensure only a single instance of the malware is active. The malware establishes persistence using Registry Run keys, Scheduled Tasks, and the Startup folder on Windows, LaunchAgent plist files on macOS, and .desktop autostart entries and crontab reboot tasks on Linux, while maintaining communication with its command and control infrastructure through TCP, WebSocket, TLS, or HTTPS. An integrated watchdog component continuously attempts to restore communication if connectivity with the command and control server is interrupted, while an optional Pastebin-based mechanism allows operators to rotate command and control infrastructure without rebuilding the malware.

The malware utilizes a broad collection of modular capabilities that provide attackers with comprehensive control over compromised systems. Researchers observed support for remote command execution, encrypted plugin delivery, credential theft, file transfer, clipboard manipulation, webcam surveillance, and fileless shellcode execution on Windows, enabling operators to dynamically expand functionality throughout an intrusion. QuimaRAT also includes an optional Binder feature that can execute an embedded payload or decoy application alongside the primary RAT process, increasing the likelihood of successful compromise while reducing user suspicion. The malware's modular Java architecture, combined with embedded Java Native Access libraries and obfuscation techniques, enables the framework to maintain a consistent codebase across multiple operating systems while complicating static detection. This combination of cross-platform persistence, dynamic plugin loading, resilient command and control communications, and extensive post-compromise capabilities allows QuimaRAT operators to maintain long-term access, perform reconnaissance, deploy additional malware, and exfiltrate sensitive information from victim environments.

# MITRE CONTEXT

- **MITRE Technique IDs:**
  - T1037.005
  - T1564.001
  - T1518.001
  - T1647
  - T1053.003
  - T1547.001
  - T1543.001
  - T1053.005

- **MITRE Technique Names:**
  - Security Software Discovery
  - Scheduled Task
  - Plist File Modification
  - Launch Agent
  - Cron
  - Registry Run Keys / Startup Folder
  - Hidden Files and Directories
  - Startup Items

- **MITRE Tactic Names:**
  - Privilege Escalation
  - Discovery
  - Execution
  - Persistence
  - Defense Evasion

# REFERENCES

1. https://www.levelblue.com/hubfs/Web/Library/Documents_pdf/Threat_Spotlight_An_In_Depth_Analysis_of_QuimaRAT.pdf