Analyst’s Brief: Moonrise RAT

By Scarlet Shark

Published: 2026-03-12 · Archived: 2026-04-05 22:50:04 UTC

3 min read

Mar 12, 2026

By Alec Dhuse

Press enter or click to view image in full size

Moonrise RAT is a 64-bit Windows binary compiled in Golang designed for stealthy persistence, information theft, and comprehensive remote control of infected Windows systems.

Key Capabilities

● **Persistent Surveillance:** Real-time keylogging, clipboard monitoring, webcam capture, and microphone access.

● **Victim Profiling:** Detection of the operating system, hostname, external IP address, and user ID.

● **Crypto-Theft:** Dedicated code designed to identify and manipulate cryptocurrency addresses, likely enabling the malware to replace a victim's wallet address with the attacker's during a transaction.

● **Interactive Control:** The malware maintains a persistent WebSocket connection, allowing attackers to push commands instantly.

● **System Sabotage:** In addition to surveillance capabilities, the malware includes disruptive functions such as triggering a Blue Screen of Death, shutting down the infected machine, and an unidentified voltage drop function.

Overview

Moonrise RAT is particularly interesting because it differs from many other malware families that rely on multiple layers of packing to evade antivirus software. Instead, it leverages the inherent complexity of the Go runtime to serve as a barrier against reverse engineering and static antivirus analysis.

The use of WebSockets for real-time, bidirectional communication is also noteworthy.

Although Moonrise RAT initially avoided static detection, its persistent WebSocket connection to a hard-coded C2 endpoint creates opportunities for network-level detection, even when the file itself may not trigger traditional antivirus alerts.

Moonrise RAT also attempts to establish a permanent foothold on infected machines. It copies itself to a hidden or less scrutinized directory, such as the user's %APPDATA% folder, often using a deceptive filename, and then creates a Run key entry in the Windows Registry to maintain persistence.

Potential Impacts

Moonrise RAT's information-stealing functionality is likely to lead to account compromises for services with active sessions or stored credentials on the infected device. Cryptocurrency theft, through manipulation of transaction destination addresses, is also a likely outcome.

Outlook

Moonrise RAT was initially detected in mid-February and had a very low detection rate. Shortly after Any.Run published its initial report on the malware, and security vendors updated their detection rules.

Get Scarlet Shark's stories in your inbox

The creators of Moonrise RAT will likely modify the malware to evade current detection methods and establish a new command-and-control infrastructure to bypass network-based threat intelligence feeds.

Detection Resources

Moonrise RAT Detection YARA Rule

```
rule Moonrise_RAT_20260311 {
  meta:
      description = "Detects Moonrise RAT malware based on unique functional and behavioral strings.
      author = "Alec Dhuse"
      date = "2026-03-12"
      hash = "082fdd964976afa6f9c5d8239f74990b24df3dfa0c95329c6e9f75d33681b9f4"
      malware = "Moonrise RAT"

    strings:

        $func1 = "fun_bsod"
        $func2 = "fun_shutdown"
        $func3 = "voltage_drop"
        $func4 = "screenshot"


        $ws1 = "websocket" ascii wide
        $ws2 = "gorilla/websocket" ascii

    condition:
        uint16(0) == 0x5A4D and
        (
            (3 of ($func*)) or
            (all of ($ws*) and 2 of ($func*))
        )
}
```

Victim Locations Based on VirusTotal Telemetry:

- Canada
- France
- Germany
- India
- Ireland
- Japan
- Netherlands
- Philippines
- Russia
- Singapore
- United Arab Emirates
- United Kingdom
- United States

Indicators of Compromise (IoCs)

Command and Control Server IPs

> 193.23.199[.]88
>
> 108.165.164[.]57

SHA-256 File Hashes

> ed5471d42bef6b32253e9c1aba49b01b8282fd096ad0957abcf1a1e27e8f7551
>
> 0a3343645c8c8cc4d83200ff351bb5a5d03e4ae6cfef902ea62963f0cf8d1849
>
> 37889bef6df21a8f4df770aaf461e99e27e695908bb2cd0f8987dc202be075ed

Tactics, Techniques, and Procedures (TTPs)

Defense Evasion

- T1027 — Obfuscated Files or Information

Discovery

- T1016 — System Network Configuration Discovery
- T1033 — System Owner/User Discovery
- T1057 — Process Discovery
- T1082 — System Information Discovery

Collection

- T1056 — Input Capture
- T1115 — Clipboard Data
- T1123 — Audio Capture
- T1125 — Video Capture

Credential Access

- T1056 — Input Capture

Command and Control

- T1071 — Application Layer Protocol

Impact

- T1657 — Financial Theft

Additional Reporting on Moonrise RAT

- https://any.run/cybersecurity-blog/moonrise-rat-detected/
- https://evalian.co.uk/inside-a-new-malware-trojan-moonrise/
