

Moonrise RAT: A New Low-Detection Threat with High-Cost Consequences

any.run/cybersecurity-blog/cybersecurity-blog/moonrise-rat-detected

ANY.RUN

February 24, 2026

Content

Recent posts

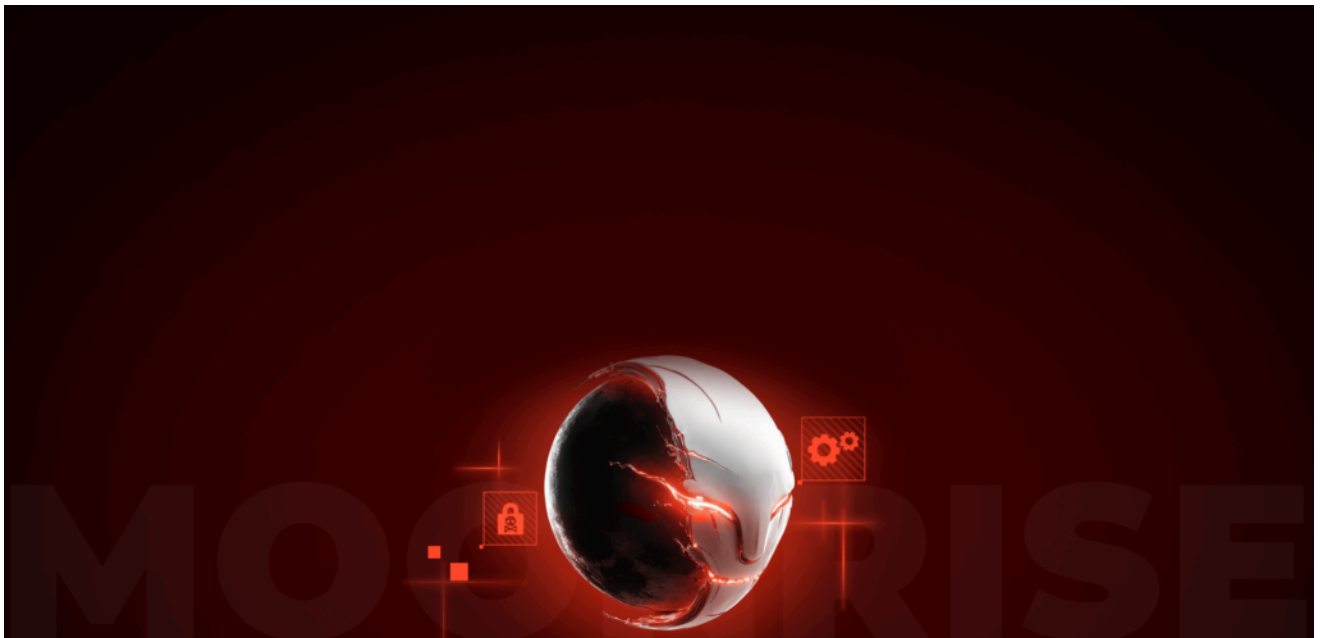


- [ANY.RUN & Splunk Enterprise: Stronger Detection, Faster Response in Your SOC](#)
[907 0](#)



- [Turn Your SOC Into a Detection Engine: Rethinking Threat Monitoring](#)

[537 0](#)



- [Moonrise RAT: A New Low-Detection Threat with High-Cost Consequences](#)

[2842 0](#)

[HomeMalware Analysis](#)

Moonrise RAT: A New Low-Detection Threat with High-Cost Consequences

Security professionals rely on early detection signals to prioritize and contain incidents. But what happens when a fully capable RAT generates none?

In a recent investigation, the [ANY.RUN](#) experts uncovered a new Go-based remote access trojan we named [Moonrise](#). At the time of analysis, it wasn't detected on VirusTotal and had no vendor signatures tied to it.

That's the problem teams can't ignore: credential theft, remote command execution, and persistence can be active while static checks stay silent. The result is slower triage, and more escalations.

Let's break down Moonrise's full attack chain and show how you can detect similar threats earlier, before they turn into longer investigations and real business impact.

Key Takeaways

Moonrise operated without early static detection, establishing active C2 communication before any vendor alerts were triggered.

The RAT supports **credential theft, remote command execution, persistence, and user monitoring**, enabling full remote control of an infected endpoint.

Silent C2 activity increases business exposure, extending dwell time and raising the risk of data loss, operational disruption, and financial impact.

Static reputation checks alone are not enough. [Behavior-based analysis](#) is critical to confirm real attacker activity quickly.

What Moonrise Means for Organizations

Moonrise isn't just a remote access tool. Its command set shows how an attacker can move from access to impact.

Credential theft and clipboard monitoring can expose passwords, session tokens, and sensitive data copied between systems.

Remote command execution and process control let operators run scripts, interfere with defenses, and manipulate business applications.

File upload and execution creates a clean path to drop additional payloads, including stealers or ransomware.

Screen capture, webcam, and microphone access can reveal what's happening inside finance workflows, admin panels, and internal communications.

Persistence and privilege-related functions increase dwell time and make removal harder.

One compromised endpoint can disrupt operations and **lead to financial and reputational damage**, especially when the malware stays below static detection thresholds long enough to expand access.

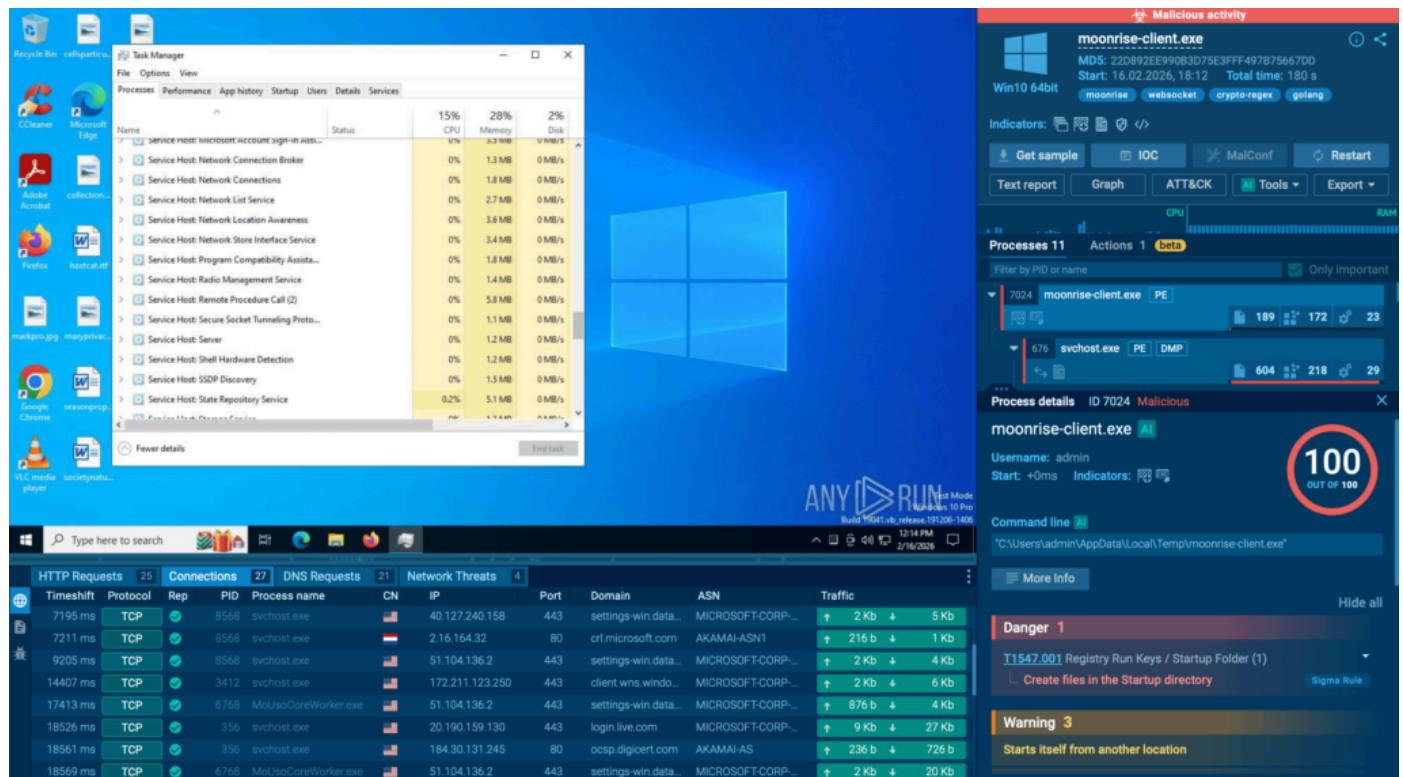
Reduce escalation and investigation costs
Detect threats earlier with behavior-first clarity

[Integrate in your SOC](#)

Attack Details Exposed: What We Observed in Execution

You can follow the full Moonrise chain in real time, from execution to C2 control, and note the behaviors you can use for detection and triage.

[Check analysis session with Moonrise](#)



Moonrise RAT detected inside ANY.RUN sandbox, revealing its full attack chain

Within minutes of execution, Moonrise established outbound communication and began responding to operator-driven commands. What looked harmless in static checks immediately revealed interactive control once behavior was observed.

Reduce investigation time from hours to minutes
Act on evidence, not assumptions

[Register now](#)

1. Session Registration and Persistent Communication

The communication begins with:

- client_hello
- connected
- ping/pong

These commands handle client identification and keep the WebSocket session alive. This confirms that the infected system is actively connected and ready to receive instructions.

At this stage, traditional static checks still show nothing suspicious. But behaviorally, the endpoint is already under remote control.

ANY RUN

```
{"type":"command","command":"screenshot"}
{"data":{"error_type":"screenshot_error","message":"no disp"}}
```

[illegible]

```
{
  "type": "command",
  "command": "process_list",
  "id": "process_list",
  "data": {}
}
```

Process listing response

[illegible]

```

{"data":{"filename":"general (ALT).bat","message":"","C:\\Users\\admin\\AppData\\Local\\Temp\\general (ALT).bat","type":"file_uploaded"}

```

```

{"type":"pong","data":{"timestamp":1771262043966}}{"type":"command","command":"clipboard_monitor_start","commandId":"clipboard_monitor_start_1771262053920_v4ywi","message":"Clipboard monitor started, success:true"}

{"type":"command","command":"clipboard_get_history","commandId":"clipboard_get_history_1771262055563_l0ikwb","data":{"list":1771262066494_wl09nc},"data":{}}

{"cameras":[{"id":"0","label":"Default Camera"}],"commandId":"webcam_list_1771262066494_wl09nc","success":true,

```

ed5471d42bef6b32253e9c1aba49b01b8282fd096ad0957abcf1a1e27e8f7551

COMMENTS

0

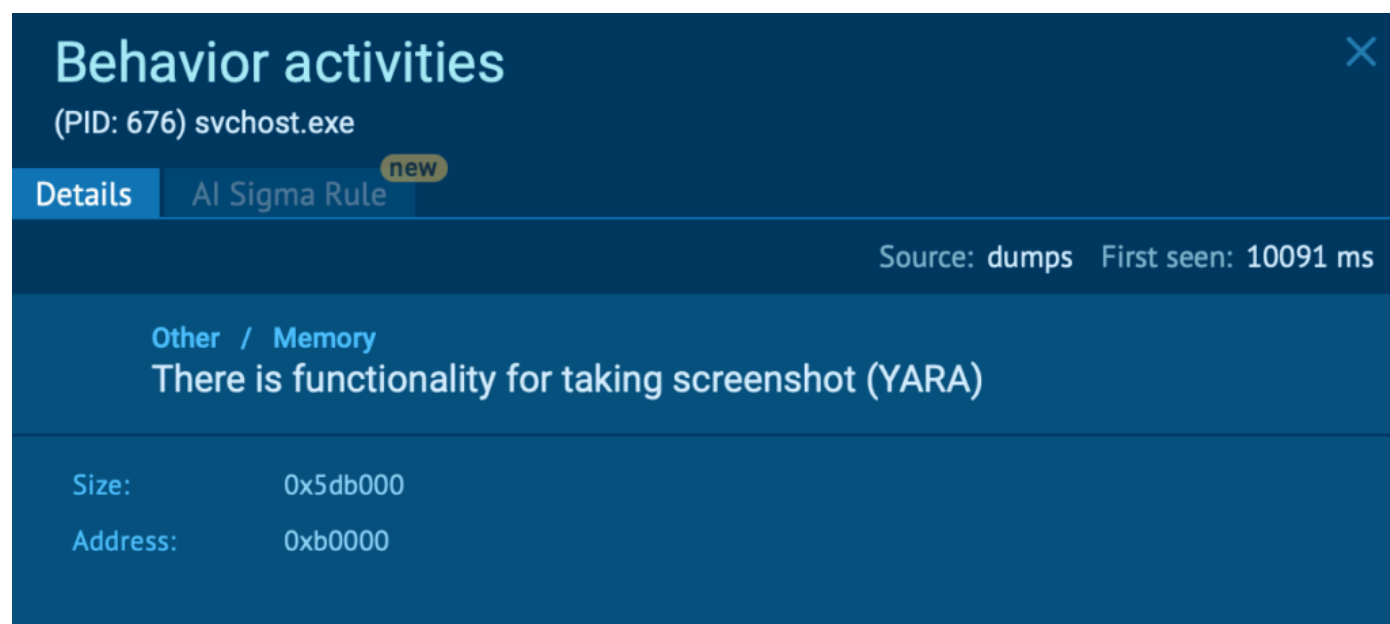
2. Visibility Into the Host Environment

Once the session is established, the operator starts requesting information about the system.

Observed commands include:

- process_list
- file_list
- webcam_list
- monitors_list
- screenshot

This allows the attacker to inspect running processes, review directory structures, identify connected displays, and check for available multimedia devices. Even when screen capture fails in a headless environment, the attempt itself signals active operator-driven interaction.



Behavior activities (PID: 676) svchost.exe

Details AI Sigma Rule ^{new}

Source: dumps First seen: 10091 ms

Other / Memory

There is functionality for taking screenshot (YARA)

Size: 0x5db000

Address: 0xb0000

YARA rule match confirming screenshot functionality inside the Moonrise process

This stage provides the attacker with enough context to determine what data is accessible and which actions to take next.

3. Direct System Interaction and Control

Moonrise supports active command execution and process manipulation:

cmd

process_kill

file_upload

file_run

file_execute

file_delete

mkdir

explorer_restart

Through these commands, the operator can run system commands remotely, terminate selected processes, upload additional payloads, execute them, modify directories, and restart system components.

Behavior activities

(PID: 676) svchost.exe

Details

AI Sigma Rule new

Source: process First seen: 157 ms

Warning / General

Starts CMD.EXE for commands execution

Image:

C:\Windows\System32\cmd.exe

Cmdline:

cmd /c ver

svchost.exe spawning cmd.exe to execute system commands inside the ANY.RUN sandbox

This shifts the attack from observation to full control. At this point, the endpoint is no longer just compromised. It can be used to deploy further tools or prepare deeper access.

4. Credential Access and Data Extraction

The sample includes commands associated with data theft and credential harvesting:

stealer

steam

file_download

keylogger_logs

clipboard_history

These functions enable collection of stored credentials, extracted files, logged keystrokes, and clipboard content. If sensitive data is copied between applications, such as passwords or financial details, it becomes accessible to the operator.

This is where technical compromise transitions into business exposure.

Reduce the risk of silent data exfiltration

Turn weak signals into clear decisions fast

[Integrate now](#)

5. Active User Monitoring

Moonrise includes extensive user interaction monitoring capabilities:

keylogger_start

keylogger_stop

keylogger_logs

input

clipboard_monitor_start

clipboard_monitor_stop

clipboard_history

clipper_get_addresses

clipper_set_address

screenshot

screen_stream_start

screen_stream_stop

webcam_capture

microphone_record

These commands allow the operator to monitor user input, track clipboard changes, capture screen content, and access audio or video devices.

The infected endpoint effectively becomes a live surveillance point.

fun_wallpaper

fun_openurl

fun_shake

fun_sound

fun_restart

fun_shutdown

fun_bsod

These commands suggest the ability to trigger visible system actions, including restarts or shutdown events, depending on operator intent.

Their presence reinforces that Moonrise provides broad remote interaction capabilities beyond silent monitoring.

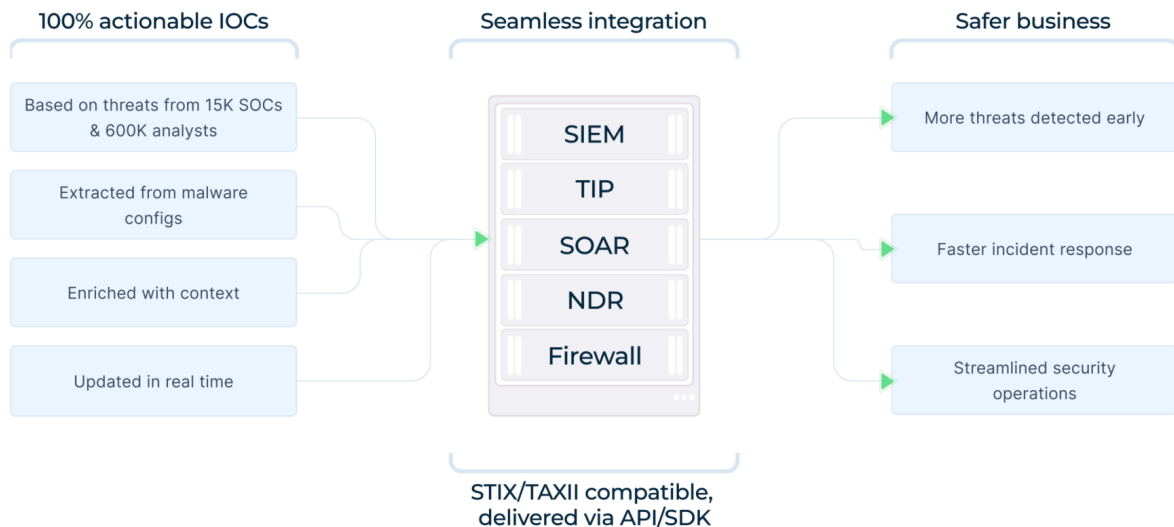
Early Detection: 3-Step Loop That Works for Stealth RATs

Moonrise is a good example of an annoying reality: sometimes a RAT shows up with no clean static verdict, no reputation you can trust, and nothing obvious to latch onto. In those cases, early detection comes down to how quickly your team can move from unclear signals to evidence-based containment.

1. Monitoring: Catch the First Weak Signal Early

A lot of RAT incidents start with infrastructure: a fresh IP, a new domain, traffic that doesn't match your baseline.

[Threat Intelligence Feeds](#) help. They continuously surface newly observed indicators and patterns based on telemetry and submissions from **15,000+ organizations and 600,000+ security professionals**.



100% actionable IOCs delivered by TI Feeds to your existing stack

For SOC managers, that means fewer blind spots in day-to-day monitoring and earlier detection of suspicious infrastructure before it becomes a bigger incident.

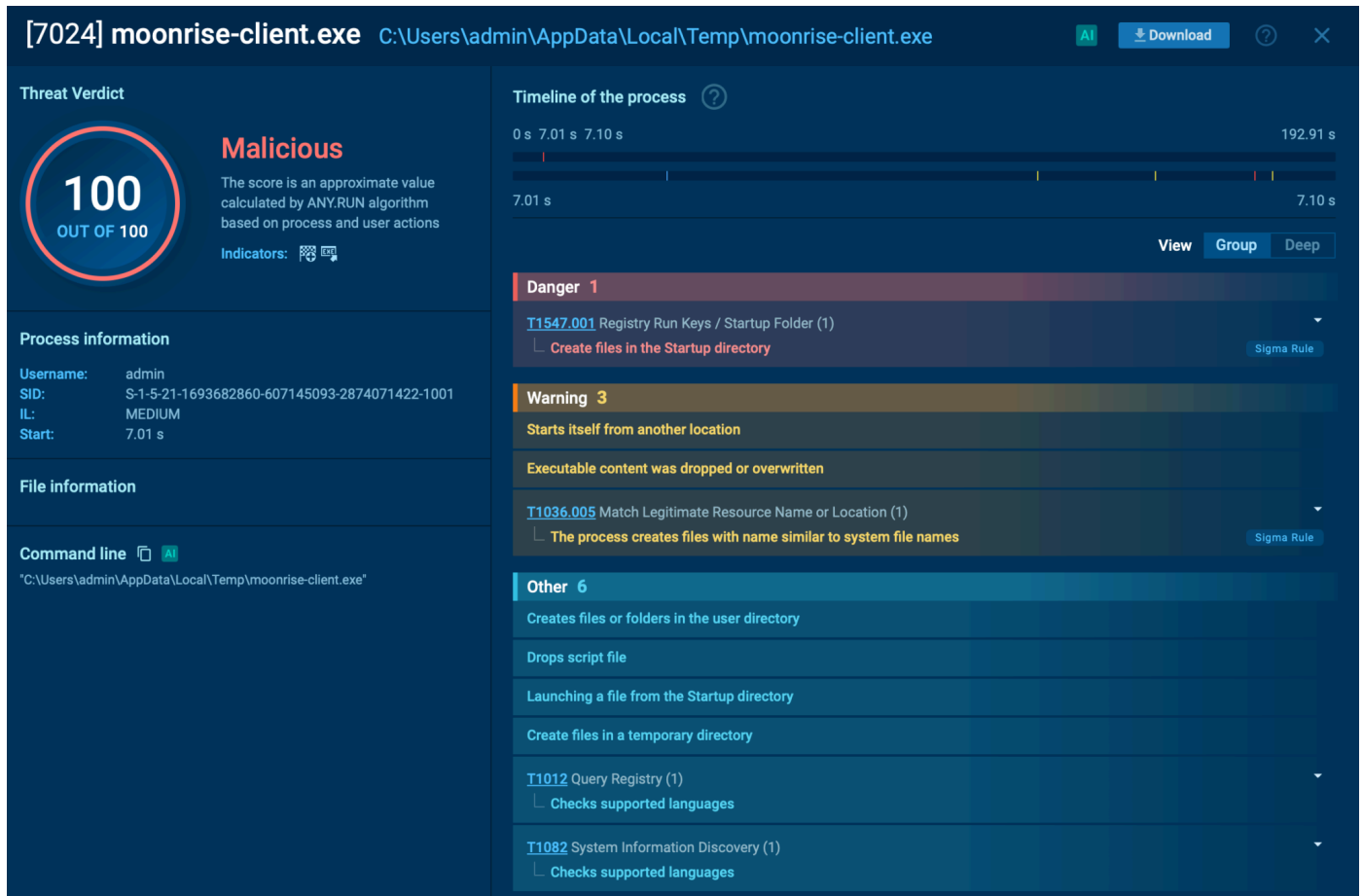
99% unique threat data for your SOC
Catch attacks early to protect your business

[Integrate TI Feeds](#)

2. Triage: Enrich Fast, Then Confirm with Behavior

When static checks don't help, teams often lose time debating severity. That's where MTTR grows and escalation pressure builds.

A cleaner path is enrich → execute → decide. Use [Threat Intelligence Lookup](#) to pull immediate context around a hash, URL, domain, or IP (relationships, related samples, historical sightings). Then run the artifact in the to confirm what it actually does in a safe environment.



ANY.RUN's sandbox detected full attack chain of Moonrise, including the implemented TTPs in a few minutes, instead of hours

This is how teams replace uncertainty with evidence, reduce unnecessary Tier-1 escalations, and contain earlier, before a RAT turns into credential loss or broader access.

74% of Fortune 100 companies
for earlier detection and faster SOC response

[Power your SOC now](#)

3. Threat Hunting: Turn One Confirmed Case into Wider Coverage

Once you confirm a RAT-like incident, the next step is making sure it doesn't repeat under a slightly different wrapper. [Threat Intelligence Lookup](#) helps you pivot from confirmed indicators to related infrastructure and nearby samples, so hunting stays tied to what's active now.

From there, you can pivot into related IPs/domains, cluster similar samples, and validate behavior in the sandbox to decide whether it's the same activity or a lookalike.

Below is an example of a TI Lookup query for the Moonrise C2 IP observed in the attack:

[destinationIP:"193.23.199.88"](#)

Lookup

YARA

License expires: Dec 14, 2026

Requests: 95 / 100

Premium

destinationIP:"193.23.199.88"

×

Search

Overview

Domains

IPs 1

URLs 1

Events 24

Files

Network threats 3

Synchronization

Analyses 14

Windows 10 Professional 64 bit

February 24, 2026 06:49

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

Windows 10 Professional 64 bit

February 24, 2026 05:15

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

Windows 10 Professional 64 bit

February 23, 2026 06:25

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

Windows 10 Professional 64 bit

February 19, 2026 13:09

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

moonrise

rat

Windows 10 Professional 64 bit

February 19, 2026 11:09

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

moonrise

rat

websocket

Windows 10 Professional 64 bit

February 19, 2026 08:59

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

moonrise

rat

websocket

Windows 10 Professional 64 bit

February 19, 2026 08:24

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

22D892EE990B3D75E3FFF497B75667DD

SHA1:

2D88CCE5BB24A768A7A60C28E46B8B1E1655FC5F

SHA256:

ED5471D42BEF6B32253E9C1ABA49B01B8282FD096AD0957ABCF1A1E27E8F7551

moonrise

rat

Windows 10 Professional 64 bit

February 18, 2026 13:48

✓

Suspicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

04F155DB6A0AB55AAC69CCBC9B1BC83

SHA1:

60B37410F9EB225A6258E3E4E7578C3AF1D8AA8

SHA256:

C7FD265823B2255729EED688A211FC3BD2192834C08E4959D1F17A0B697CD5E

moonrise

crypto-regex

golang

websocket

Windows 10 Professional 64 bit

February 16, 2026 19:01

✓

Malicious activity

moonrise-client.exe

PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS...

MD5:

04F155DB6A0AB55AAC69CCBC9B1BC83

SHA1:

60B37410F9EB225A6258E3E4E7578C3AF1D8AA8

SHA256:

C7FD265823B2255729EED688A211FC3BD2192834C08E4959D1F17A0B697CD5E

moonrise

websocket

crypto-regex

golang

TI Lookup displays sandbox analyses related to the IP address used in the Moonrise attack

When these three motions run as a loop, monitoring, fast triage, and targeted hunting, stealth RATs stop being “late discoveries” and become manageable security events with lower response cost and less business exposure.

Conclusion: Reducing Exposure Starts with Faster Clarity

Moonrise is a reminder that the biggest risk isn’t the RAT itself but the time lost before it’s clearly identified. When static checks stay silent, attackers can steal credentials, stage more payloads, and lock in persistence while teams are still debating severity.

Reducing exposure comes down to one thing: faster clarity. Feed fresh infrastructure signals into monitoring, enrich quickly with TI Lookup, and confirm behavior in the sandbox before the case grows into a costly incident.

[Bring speed and clarity to your SOC with ANY.RUN →](#)

[ANY.RUN](#), a leading provider of interactive [malware analysis](#) and threat intelligence solutions, fits naturally into modern SOC workflows and supports investigations from initial alert to final containment.

It allows teams to safely execute suspicious files and URLs to observe real behavior, enrich indicators with immediate context through [TI Lookup](#), and continuously monitor emerging infrastructure using [Threat Intelligence Feeds](#). Together, these capabilities help reduce uncertainty, accelerate triage, and limit unnecessary escalations.

Today, more than 600,000 security professionals across 15,000+ organizations rely on ANY.RUN to make faster decisions, strengthen detection coverage, and stay ahead of evolving phishing and malware campaigns.

To stay informed about newly discovered threats and real-world attack analysis, follow ANY.RUN’s team on [LinkedIn](#) and [X](#), where weekly updates highlight the latest research, detections, and investigation insights.

Indicators of Compromise (IOCs)

193[.]23[.]199[.]88
c7fd265b23b2255729eed688a211f8c3bd2192834c00e4959d1f17a0b697cd5e
8a422b8c4c6f9a183848f8d3d95ace69abb870549b593c080946eaed9e5457ad
7609c7ab10f9ecc08824db6e3c3fa5cbdd0dff2555276e216abe9eebfb80f59b
Ed5471d42bef6b32253e9c1aba49b01b8282fd096ad0957abcf1a1e27e8f7551
082fdd964976afa6f9c5d8239f74990b24df3dfa0c95329c6e9f75d33681b9f4
8d7c1bbdb6a8bf074db7fc1185ffd59af0faffb08e0eb46a373c948147787268

[ANYRUN cybersecurity malware analysis](#)

What do you think about this post?

3 answers

- Awful
- Average
- Great

Save my name and email in this browser for the next time I comment.

0 comments