Threat Intelligence & Malware Analysis Report: Yellow Cockatoo (SolarMarker) RAT

Analyst: Mduduzi William Radebe

Date: 08 February 2026

Platform: CyberDefenders

Vulnerability Type: Remote Access Trojan (RAT) / Search Redirection

Severity: High

1. Executive Summary

A comprehensive analysis was conducted on a malicious artifact identified during a routine security audit at GlobalTech Industries. Through the use of threat intelligence platforms and behavioral analysis, the sample was attributed to the **Yellow Cockatoo** (also known as **SolarMarker** or **Jupyter**) malware family. This malware specializes in search engine poisoning to trick users into downloading high-risk payloads. Once executed, it establishes a persistent presence on the host and communicates with a Command and Control (C2) server to facilitate data exfiltration.

2. Project Objective

The objective of this investigation was to:

- Identify the specific malware family and its operational tactics.
- Extract static file artifacts (PE Headers, Timestamps, and GUID-based filenames).
- Determine the timeline of the attack from creation to community detection.
- Map the malware's persistence mechanisms and network infrastructure.

3. Tools & Intelligence Sources

- **VirusTotal (OSINT):** Used for hash lookups, community reports, and static file analysis (PE Headers).
- **Red Canary (Threat Intel Blog):** Utilized for deep-dive behavioral mapping and identifying specific file-dropped artifacts.
- **Any.Run (Sandbox Analysis):** Used to observe live process execution and network callback behavior.

4. Investigative Methodology (Step-by-Step)

Phase 1: Attribution & Community Intelligence

Action: I submitted the file hash to **VirusTotal** and reviewed the **Community** tab.

Finding: Analysts across the community confirmed the sample belongs to the **Yellow Cockatoo RAT** family.

Context: This group is known for its sophisticated use of .NET and PowerShell to evade traditional antivirus detection.

Phase 2: Static Analysis (Digital DNA)

Action: I navigated to the **Details** tab in VirusTotal to inspect the "Portable Executable (PE) Info."

Finding:

- **Internal Filename:** The malware utilized a GUID-based filename: 111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll.
- **Compilation Timestamp:** The malware was "born" on **2020-09-24 at 18:26**. **Significance:** Identifying the compilation time allows us to see how long a "zero-day" threat existed before security vendors created a signature for it.

Phase 3: Threat Timeline Analysis

Action: I cross-referenced the compilation date with the **History** section of the report.

Finding: The malware was first submitted to VirusTotal on **2020-10-15 at 02:47**.

Analyst Note: There was a **21-day gap** between creation and discovery, representing a significant "window of vulnerability" for the organization.

Phase 4: Behavioral Intelligence & C2 Discovery

Action: Recognizing that the sample had encrypted strings, I turned to **Red Canary's technical blog** to find specific artifacts that the malware "drops" after infection.

Finding: * **Persistence Artifact:** The malware drops a file named solarmarker.dat in the user's AppData directory.

- **C2 Infrastructure:** Through network analysis and OSINT documentation, the Command and Control server was identified as **hxxps://gogohid[.]com**.

5. Technical Findings Summary

Metric	Discovery
Malware Family	Yellow Cockatoo (SolarMarker)
Primary Filename	111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll
Compilation Date	2020-09-24 18:26
Initial VT Submission	2020-10-15 02:47
Dropped File (.dat)	solarmarker.dat
C2 Server	gogohid[.]com

6. Analyst Reflections

Struggles & Challenges

- **Navigating PE Headers:** As a beginner, reading the "Portable Executable" section was intimidating. I had to learn that the "Header" information is where the computer hides the true "creation date" of a file, even if the file's external properties were changed.
- **Identifying Redirection:** It was challenging to understand how a "search redirect" leads to a RAT. I had to research how hackers use SEO (Search Engine Optimization) to push their malicious websites to the top of Google search results.

Lessons Learned

- **The Power of OSINT:** Not every answer is in the code. Using external blogs like Red Canary proved that collaborating with the wider security community is essential for solving complex cases.
- **History Matters:** Comparing the compilation date vs. the submission date taught me that attackers often wait weeks before launching a campaign to ensure their malware stays "silent."

7. Recommended Mitigation

1. **Network Level:** Block the domain gogohid.com at the perimeter firewall.
2. **Endpoint Level:** Create an EDR (Endpoint Detection and Response) rule to flag any .dat file creations within the AppData folder that are not associated with known applications.

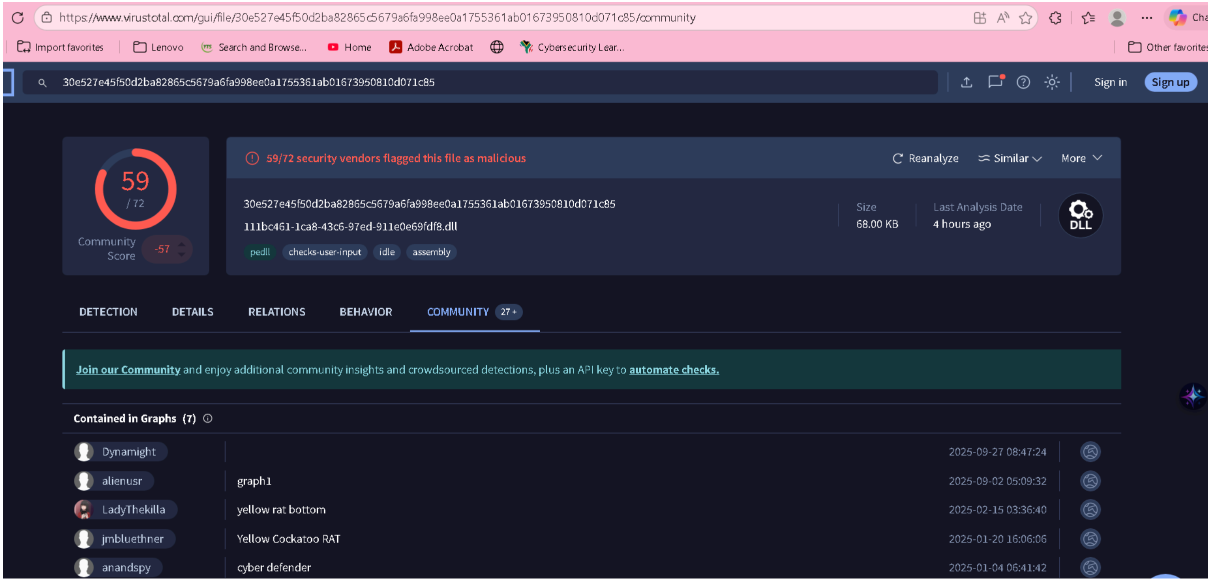
3. **User Awareness:** Train employees to verify the URL of any site asking them to download "updates" or "invoices," especially if redirected from a search engine.

Analyst Signature: Mduduzi William Radebe

Date: February 8, 2026

Screenshots and Notes

Q1:
Virus total > Under community Tab > Answer =Yellow Cockatoo RAT



59/72 security vendors flagged this file as malicious

30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85
111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll

pedll checks-user-input idle assembly

Size 68.00 KB

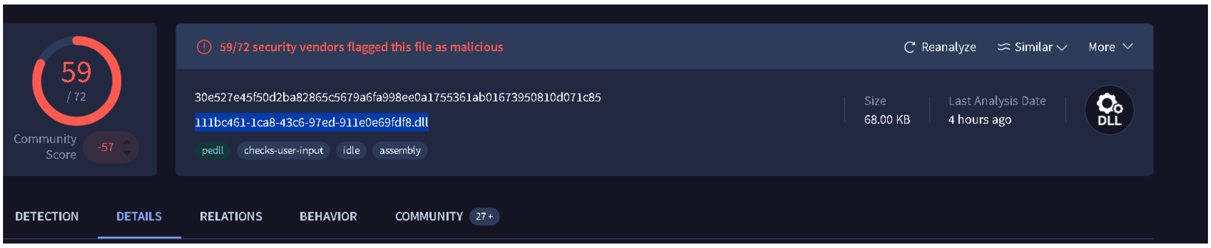
Last Analysis Date 4 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contained in Graphs (7)

Dynamight		2025-09-27 08:47:24
alienusr	graph1	2025-09-02 05:09:32
LadyThekilla	yellow rat bottom	2025-02-15 03:36:40
jmbluethner	Yellow Cockatoo RAT	2025-01-20 16:06:06
anandspy	cyber defender	2025-01-04 06:41:42

Q2:
Virus total > Under details > Answer: 111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll



59/72 security vendors flagged this file as malicious

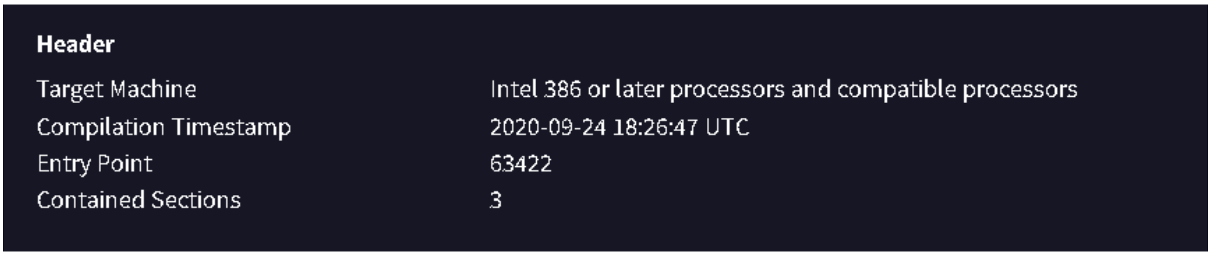
30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85
111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll

pedll checks-user-input idle assembly

Size 68.00 KB

Last Analysis Date 4 hours ago

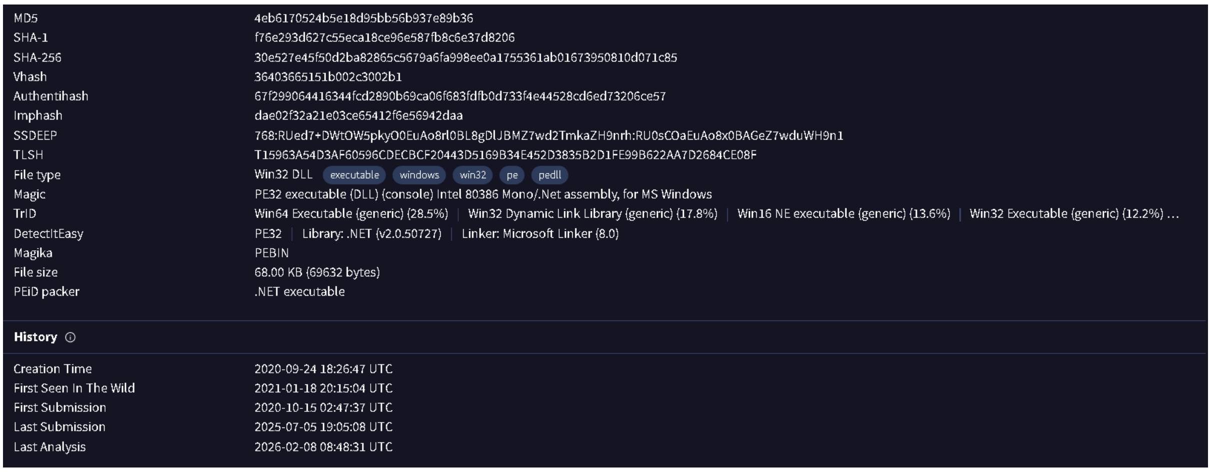
Q3:
compilation timestamp of the malware = under details > Portable Executable Info > Header >
Answer: 2020-09-24 18:26



Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2020-09-24 18:26:47 UTC
Entry Point	63422
Contained Sections	3

Q4:
first submitted to VirusTotal = Detail > History > Answer =
2020-10-15 02:47

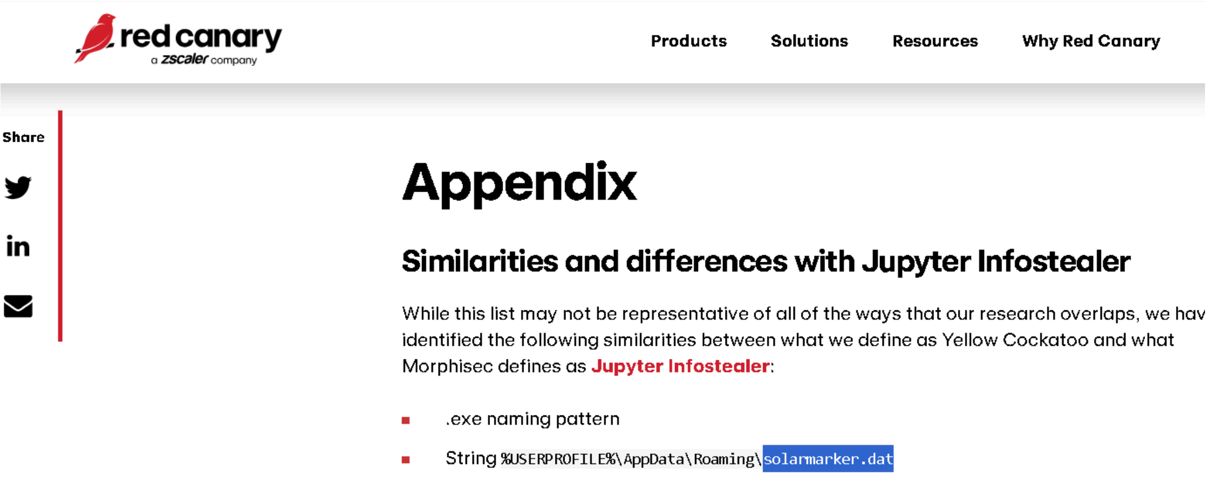


MD5	4eb6170524b5e18d95bb56b937e89b36
SHA-1	f76e293d627c55eca18ce96e587fb8c6e37d8206
SHA-256	30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85
Vhash	36403665151b002c3002b1
Authentihash	67f299064416344fcd2890b69ca06f683fdfb0d733f4e44528cd6ed73206ce57
Imphash	dae02f32a21e03ce65412f6e56942daa
SSDEEP	768:RUed7+DWtOW5pkyO0EuAo8rl0BL8gDlJBMZ7wd2TmkaZH9nrh:RU0sCOaEuAo8x0BAGeZ7wduWH9n1
TLSH	T15963A54D3AF60596CDECBCF20443D5169B34E452D3835B2D1FE99B622AA7D2684CE08F
File type	Win32 DLL executable windows win32 pe pedll
Magic	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Win64 Executable (generic) (28.5%) | Win32 Dynamic Link Library (generic) (17.8%) | Win16 NE executable (generic) (13.6%) | Win32 Executable (generic) (12.2%) …
DetectItEasy	PE32 | Library: .NET (v2.0.50727) | Linker: Microsoft Linker (8.0)
Magika	PEBIN
File size	68.00 KB (69632 bytes)
PEiD packer	.NET executable

History ⓘ

Creation Time	2020-09-24 18:26:47 UTC
First Seen In The Wild	2021-01-18 20:15:04 UTC
First Submission	2020-10-15 02:47:37 UTC
Last Submission	2025-07-05 19:05:08 UTC
Last Analysis	2026-02-08 08:48:31 UTC

Q5
name of the .dat file that the malware dropped in the AppData folder = Under Red canary https://redcanary.com/blog/threat-intelligence/yellow-cockatoo/ > under the heading Appendix > answer = solarmarker.dat



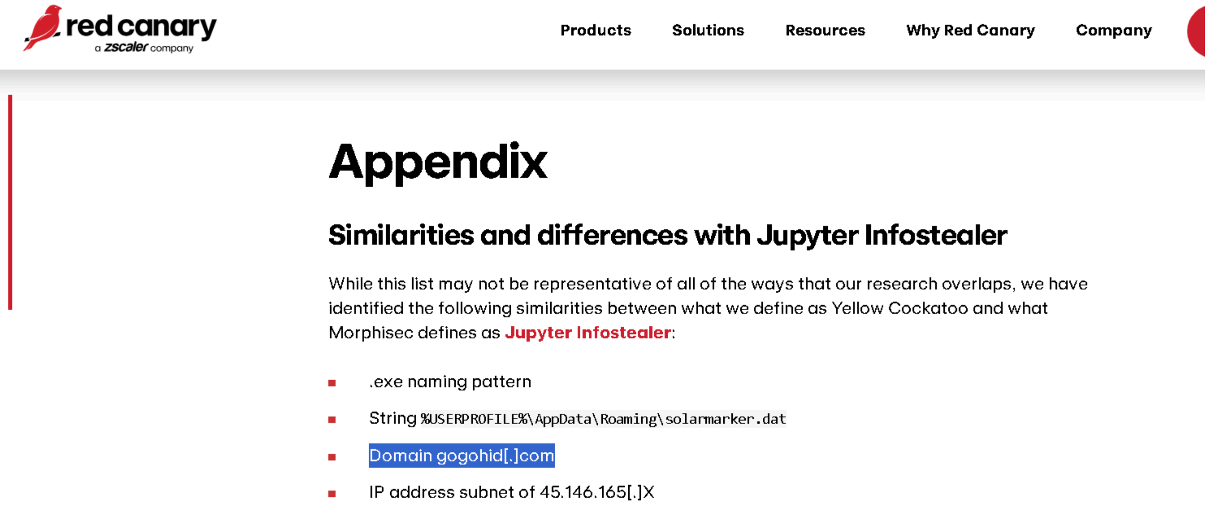
Appendix

Similarities and differences with Jupyter Infostealer

While this list may not be representative of all of the ways that our research overlaps, we hav identified the following similarities between what we define as Yellow Cockatoo and what Morphisec defines as **Jupyter Infostealer**:

- .exe naming pattern
- String `%USERPROFILE%\AppData\Roaming\solarmarker.dat`

Q6
the C2 server that the malware is communicating with = nder Red canary https://redcanary.com/blog/threat-intelligence/yellow-cockatoo/ > under the heading Appendix > answer = https://gogohid[.]com



Appendix

Similarities and differences with Jupyter Infostealer

While this list may not be representative of all of the ways that our research overlaps, we have identified the following similarities between what we define as Yellow Cockatoo and what Morphisec defines as **Jupyter Infostealer**:

- .exe naming pattern
- String `%USERPROFILE%\AppData\Roaming\solarmarker.dat`
- Domain gogohid[.]com
- IP address subnet of 45.146.165[.]X