

c-b.io | RE // DFIR // CTF

Archived: 2026-04-05 19:55:29 UTC

Welcome to Humpty's blog!

Security Research & Analysis

Hey there! Glad to see you here. I go by Humpty, some know me by Tony. This blog aims at documenting my Reverse Engineering & DFIR journey as I stumble my way through malware and funky logs.

I also run a small DFIR community! You can learn more by going to [irchaos.club](#) or by joining our Discord server at the link below.

Here are my socials:

- [Discord — Join IRCC!](#)
- [Twitter](#)
- [BlueSky](#)
- [LinkedIn](#)

Hope you enjoy! - Humpty

8 Cases

29 IOCs

19 MITRE Techniques

3 Threat Actors

| Severity | Case ID | Title | Status | Category | Threat Actor | MITRE | Created | Assignee |
|----------|----------------|---|--------|--------------------------|--------------|---|------------|------------------|
| high | CASE-2026-0404 | Cloudy With A Chance Of Compromise: How A Skid Ransoms Your Buckets | Closed | SOC Engineering / Guides | N/A | T1486 T1485 T1530 T1580 T1059.006 | 2026-04-04 | H Humpty/Tony |
| info | CASE-2026-0328 | does-not-exist-bucket exists now and it's mine | Closed | SOC Engineering / Guides | N/A | | 2026-03-28 | H Humpty/Tony |
| info | CASE-2026- | Getting SaaS with | Closed | SOC Engineering | N/A | | 2026-01-25 | H |

| Severity | Case ID | Title | Status | Category | Threat Actor | MITRE | Created | Assignee |
|----------|----------------|---|--------|----------------------------|--------------------------------|----------------------------------|------------|------------------|
| | 0125 | SIEMs — Introduction | | / Guides | | | | Humpty/Tony |
| critical | CASE-2025-0720 | Install Linters, Get Malware — DevSecOps Speedrun Edition | Closed | Supply Chain / Stealer | Unknown | T1195 T1059 T1027 T1056 | 2025-07-20 | H Humpty/Tony |
| critical | CASE-2024-0815 | Supper is served | Closed | Malware Analysis / RAT | Vanilla Tempest / Vice Society | T1059 T1071 T1140 T1573 | 2024-08-15 | H Humpty/Tony |
| low | CASE-2024-0714 | Threat hunting for shits and giggles | Closed | Threat Hunting | N/A | | 2024-07-14 | H Humpty/Tony |
| medium | CASE-2024-0610 | Analyzing the RedTiger Malware Stealer | Closed | Malware Analysis / Stealer | Unknown (script kiddie) | T1555 T1539 T1082 | 2024-06-10 | H Humpty/Tony |
| medium | CASE-2024-0522 | Dissecting a fresh BlankGrabber sample | Closed | Malware Analysis / Stealer | Unknown (script kiddie) | T1055 T1497 T1005 T1125 | 2024-05-22 | H Humpty/Tony |

[CASE-2026-0404 high](#)

[Cloudy With A Chance Of Compromise: How A Skid Ransoms Your Buckets](#)

[Closed SOC Engineering / Guides](#)

[Preface If you spend any amount of time in infosec circles, you'll notice that the vast majority of offensive research is still centered around ...](#)

[2026-04-04](#)

[T1486 T1485 T1530](#)

[CASE-2026-0328 info](#)

[does-not-exist-bucket exists now and it's mine](#)

[Closed SOC Engineering / Guides](#)

[As someone who's got the great misfortune of working very closely with Cloud providers \(namely AWS, Azure & GCP, the unholy trinity\)...](#)

[CASE-2026-0125 info](#)

[Getting SaaSy with SIEMs — Introduction](#)

[Closed SOC Engineering / Guides](#)

[Welcome! It's so good to finally have a SOC analyst, we've got so much work to do! I know this will be a lot for you as a junior since it's all we ...](#)

[CASE-2025-0720 critical](#)

[Install Linters, Get Malware — DevSecOps Speedrun Edition](#)

[Closed Supply Chain / Stealer](#)

[Recommend song to listen to while reading: If you find something off with what I say, please let me know. I'll gladly amend my content and ...](#)

[2025-07-20](#)

[T1195 T1059 T1027](#)

[CASE-2024-0815 critical](#)

[Supper is served](#)

[Closed Malware Analysis / RAT](#)

[Recommend song to listen to while reading: If you find something off with what I say, please let me know. I'll gladly amend my content and ...](#)

[2024-08-15](#)

[T1059 T1071 T1140](#)

[CASE-2024-0714 low](#)

[Threat hunting for shits and giggles](#)

[Closed Threat Hunting](#)

[I'll start by saying this post is not endorsed by hunt.io. I just happen to be a really big fan of what they're doing. Some hackers suck ...](#)

[CASE-2024-0610 medium](#)

[Analyzing the RedTiger Malware Stealer](#)

[Closed Malware Analysis / Stealer](#)

[Today we'll dive into a fresh malware stealer dubbed RedTiger, a sample targeting personal user data, particularly Discord tokens, ...](#)

[2024-06-10](#)

[T1555 T1539 T1082](#)

[CASE-2024-0522 medium](#)

[Dissecting a fresh BlankGrabber sample](#)

[Closed Malware Analysis / Stealer](#)

[BlankGrabber is nothing new. It's been documented by multiple companies such as ThreatMon, K7Security and has even had it's source code ...](#)

[2024-05-22](#)

[T1055 T1497 T1005](#)

Source: <https://c-b.io/2025-02-15+-+Dissecting+a+fresh+BlankGrabber+sample>