



[← Blog](#)

July 27, 2024

5 min read

Dark Atlas Squad

Share

Medusa Ransomware Group’s OPSEC Failure: Infiltrating Their Cloud Storage

INTRODUCTION

In the evolving threat landscape, threat actors and ransomware groups continually adapt and refine their methodologies to execute data exfiltration operations for either espionage or extortion purposes.

At BuguardHUMINT Unit “Dark Atlas Squad”, we recently responded to a ransomware incident carried out by Medusa Ransomware Group. Their OPSEC failure allowed us to infiltrate their cloud account for a certain amount of time and access the data they had been exfiltrating over time.

In this case, Medusa Group utilized a method to exfiltrate data from the victim to their cloud storage.

Rclone supports over 70 cloud providers, making it a popular tool used by ransomware groups. Normally, ransomware groups, when accessing the configuration file, use a hardcoded endpoint.

OPSEC FAIL

During our investigation, We observed that the ransomware group used a hardcoded endpoint to access the configuration file.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Deny

Allow Selection

Allow all

Page 1 of 8

DARKATLAS

| Download | Name | Size | Mode | mtime | ctime | mtime | ctime | mtime |
|----------|------------|------|----------------|----------------------|----------------------|----------------------|----------------------|-------|
| | conf.txt | | 211 -rwxr-xr-x | 2023-11-07T14:24:21Z | 2024-01-15T17:08:57Z | 2024-01-15T17:09:51Z | 2024-01-15T17:08:57Z | |
| | Programs | | 0 drwxr-xr-x | 2024-01-21T09:37:33Z | 2024-01-21T09:37:33Z | 2024-01-21T09:37:33Z | 2012-07-26T08:04:57Z | |
| | rc1one.exe | 46Mb | -rwxr-xr-x | 2022-12-23T17:27:29Z | 2024-01-15T17:07:56Z | 2024-01-15T17:09:51Z | 2024-01-15T17:07:56Z | |

10253050

Showing 1 to 3 of 3

<0>Goto Page

Rclone offers two options for users to set their configuration: either by passing a configuration file or through shell interactive mode. In this case, the former was used.

Interestingly, upon inspecting the conf.txt file located in the same directory as Rclone, we observed that the actor utilized the put.io service to exfiltrate data from the DC.

conf

FileEditView

```
[put2]
type = putio
token = {"access_token":"JP5FJHRA6KSU30PQ7OQM","expiry":"0001-01-01T00:00:00Z"}

[put]
type = putio
token = {"access_token":"4QY7754BSVNWIBYMWKD2","expiry":"0001-01-01T00:00:00Z"}
```

EXPLOITATION AND RECOVERY

Upon identifying the put.io token, we reviewed the put.io API documentation. We discovered that full authentication required a client_id and client_secret, which we did not have.

SMARTBEAR
SwaggerHub

Log In

GET

/account/info

Get account info

GET

/account/settings

Get account settings

files

Manage your files

GET

/files/list

List files and their properties

POST

/files/list/continue

Fetch remaining files via cursor

GET

/files/search

Search your and your friends' files

POST

/files/search/continue

Fetch rest of the search results

POST

/files/create-folder

Create new folder

POST

/files/rename

Rename file

POST

/files/move

Move files

POST

/files/{id}/mp4

GET

/files/{id}/mp4

GET

/files/{id}/subti

GET

/files/{id}/subti

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Deny

Allow Selection

Allow all



Home

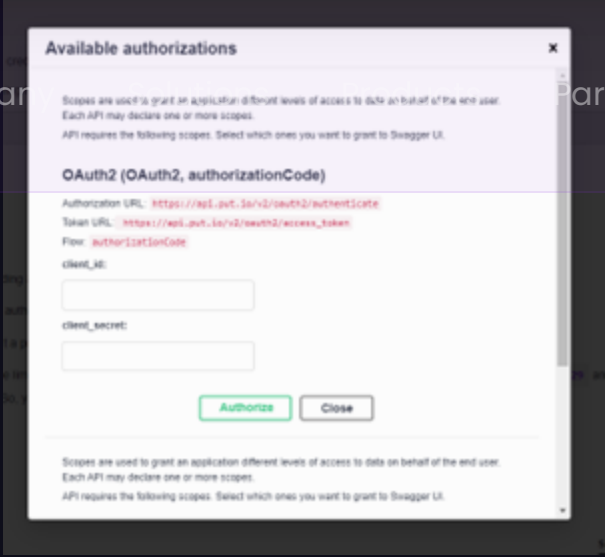
Compare

Partners

Pricing

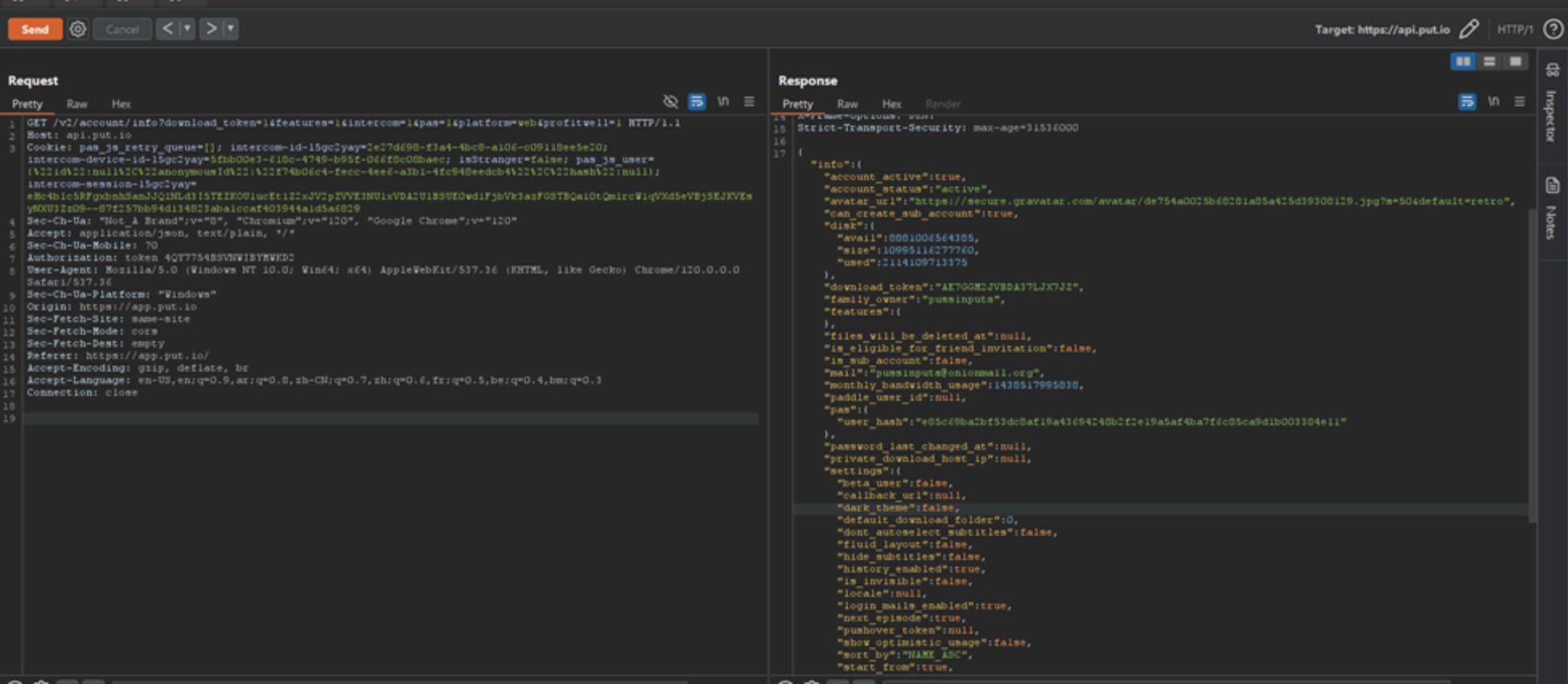
Blog

Get Started



Instead of using the official API, we explored the application as regular users and found that a single token could fully authenticate us. Using Burp Suite, we replaced our token with Medusa’s token, gaining full access to their cloud repositories.

The email associated with their account was “pussinputs@onionmail.org”.



This access allowed us to see all the exfiltrated data from victims, including the Kansas City Area Transportation Authority (KCATA).



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.



Necessary



Preferences



Statistics



Marketing

Deny

Allow Selection

Allow all



[Home](#)

[Company](#)

[Solutions](#)

[Products](#)

[Partners](#)

[Pricing](#)

[Blog](#)

[Get Started](#)

Then, we started re-capturing our customers’ stolen data by creating zips and downloading them.

We wanted to do the same for our customers.
We automated this process using

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.



Necessary !



Preferences !



Statistics !



Marketing !

Deny

Allow Selection

Allow all



[Home](#)

[Company](#)

[Solutions](#)

[Products](#)

[Partners](#)

[Pricing](#)

[Blog](#)

[Get Started](#)

Once we did this, we started to delete some sensitive files belonging to the victims.

We contacted as many victims as possible and helped them to complete the recovery process.

Finally, Dark Atlas Squad crafted a sigma rule to help detect such incidents inside your network.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.



Necessary !



Preferences !



Statistics !



Marketing !

Deny

Allow Selection

Allow all



```
title: DNS Query To Put.io
id: S1563Net-6951-4912-8516-308b0dfffd3c3
status: experimental
description: Detects DNS queries for subdomains related to Put.io sharing website
references:
  - Internal Case
author: Omar Khaled (beacon_exe)
date: 2024/02/28
logsource:
  product: windows
  service: dns-client
definition: 'Requirements: Microsoft-Windows-DNS Client Events/Operational Event Log must be enabled/collected in order to detect'
detection:
  selection:
    EventID: 3008
    QueryName|contains:
      - 'api.put.io'
      - 'upload.put.io'
      - 's111.put.io'
  condition: selection
falsepositives:
  - Legitimate DNS queries and usage of Put.io
level: medium
```

That’s it for today. Thank you for reading! Shout out to our beacon_exe & GeneralEG for this research.

Stay safe, and if you ever face ransomware or a data breach, Email us at Hello@Darkatlas.io!

Hashtags

- DarkWeb
- OPSEC Failure
- Ransomware

Share



Author

Dark Atlas Squad

Leave A Comment

Name


Work Email


This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

- ☒ Necessary
- ☒ Preferences
- ☒ Statistics
- ☒ Marketing

Deny Allow Selection Allow all


 Comment ...
[Home](#) [Company](#) [Solutions](#) [Products](#) [Partners](#) [Pricing](#) [Blog](#) [Get Started](#)

[Send](#) 

Comments

No Comment! Be the first one.

Subscribe
New Security Updates Weekly!

Enter your email 

DARKATLAS

Call us

+1 (702) 381-9571

Send to us

info@darkatlas.io

Social Media

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary !

Preferences !

Statistics !

Marketing !

Deny

Allow Selection

Allow all

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

☒

Necessary 

☒

Preferences 

☒

Statistics 

☒

Marketing 

Deny

Allow Selection

Allow all