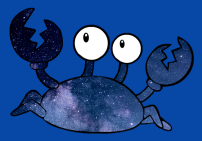
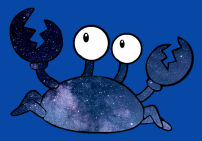
Breach Detection at Scale

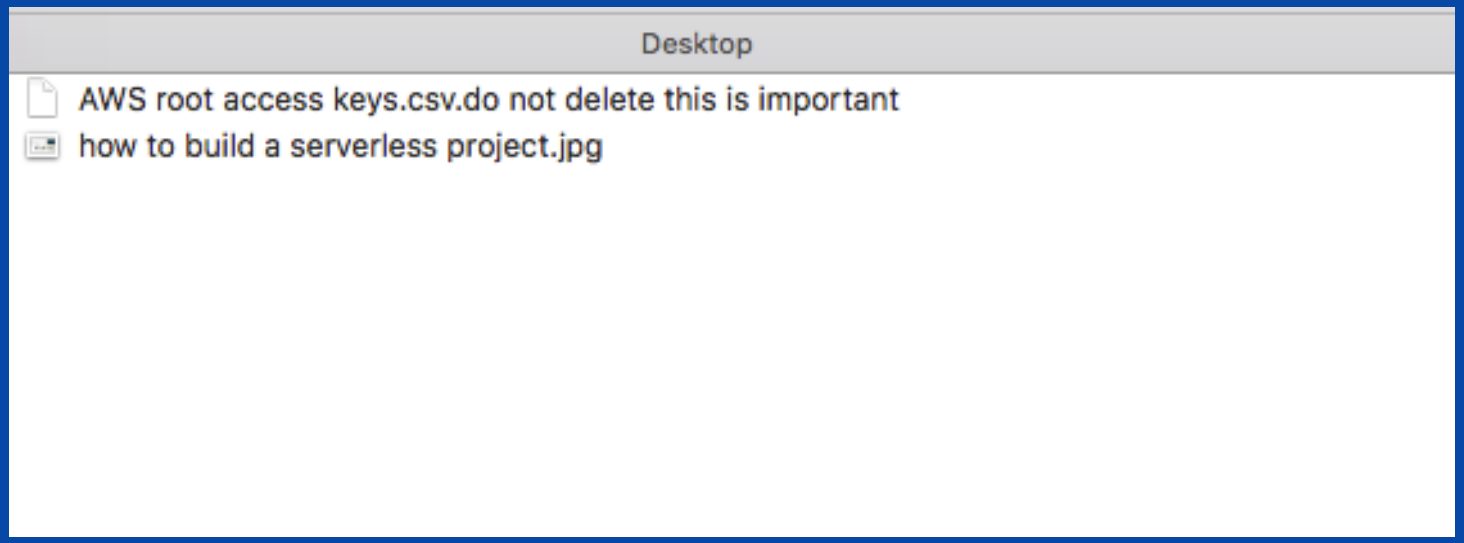
with AWS honey tokens

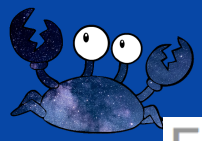
DAN BOURKE & DANIEL GRZELAK | ATLASSIAN SECURITY



AWS keys




Desktop
AWS root access keys.csv.do not delete this is important
how to build a serverless project.jpg

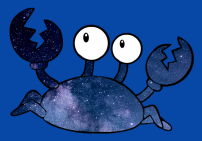


Edit SpaceCrabStack-ManagementStack-1A70CI2OFS2TP-TokenPolicy-14X81MJ0PBOO1

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Visual editor | JSON | Import managed policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```



Canarytokens by Thinkst

What is this and why should I care?

AWS keys

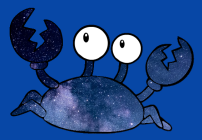
Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered, like: like AWS keys placed on Jim's laptop

Fill in the fields above

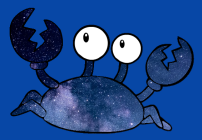
Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. **Know. When it matters.**

This slide is unsolicited advertising. Presenter was not paid for this slide. Filmed on a closed

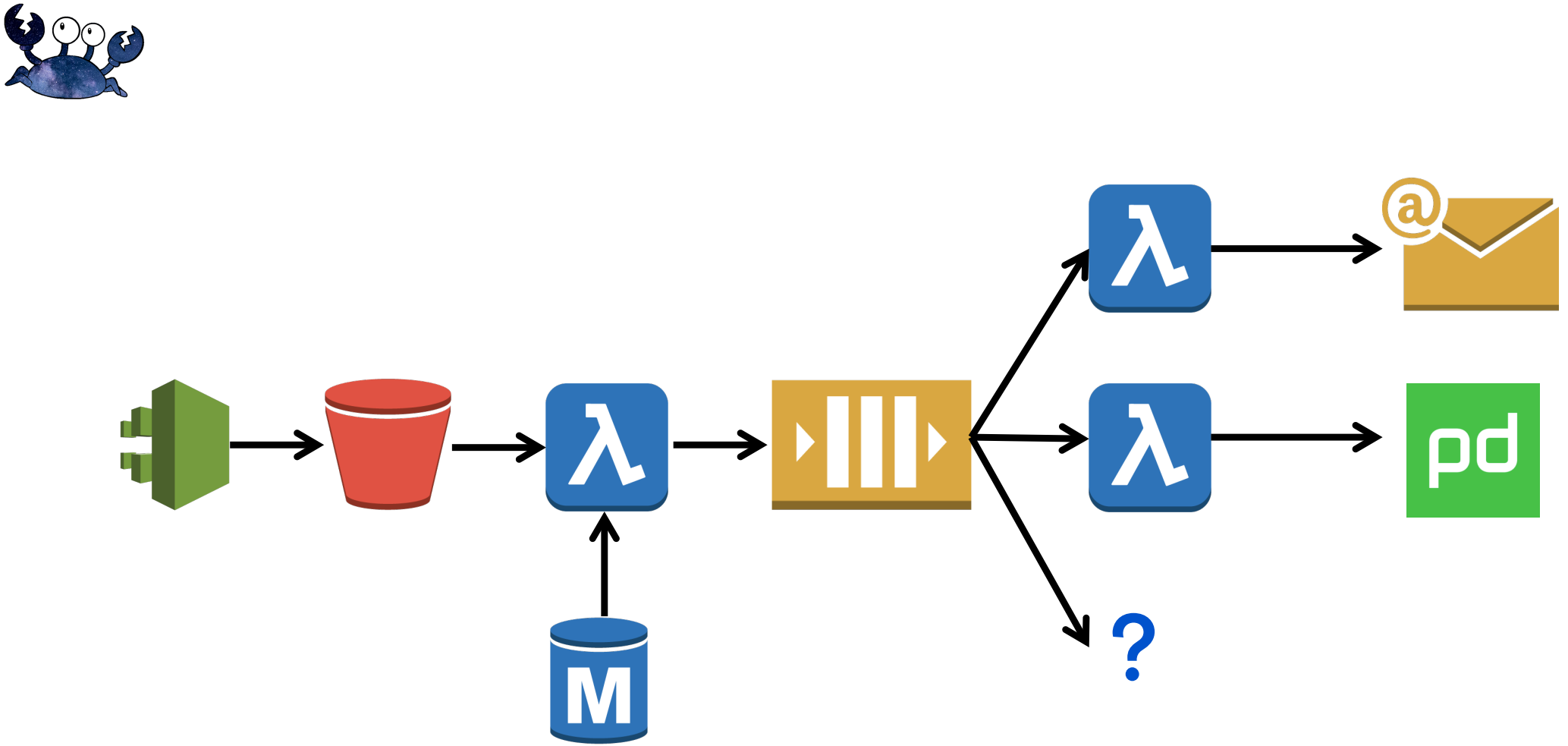


What if you want over 9000?

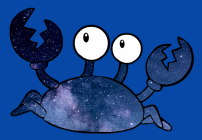
Security Advice: But less than 10,000



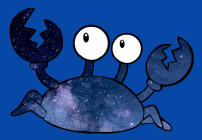
Security Advice: The space is in the crab.


M
?
pd

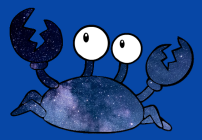

MONITOR ALL THE THINGS!



You may have some questions



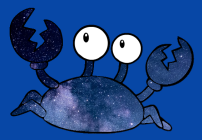
How do I set this up?



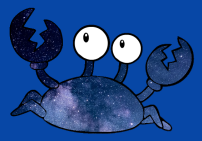
https://bitbucket.org/asecurityteam/spacecrab

```
$ python manager.py
```

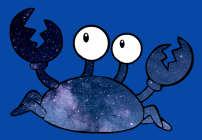

```
Welcome to Project SPACECRAB setup.
We'll begin constructing spacecrab infrastructure shortly,
but first we'll need to collect some data.


In order to secure your SPACECRAB infrastructure, we will need to limit access to a certain user or role
You are currently authenticated as:

arn:aws:iam::012345678901:role/AQUASTREAM-SysAdmin
Would you like to use arn:aws:iam::012345678901:role/AQUASTREAM-SysAdmin as your admin role? Y/n:

We'll need a path, which will be part of the generated token's ARNs.
The path must start and end with /
Please enter a "Path" for your users (defaults to /SpaceCrab/): /SpaceCrab/

We'll use the path "/SpaceCrab/", is this ok? Y/n:

Would you like to send alerts to PagerDuty? Y/n: y


We will need a Pagerduty Events API v2 integration key for this alert to work.
Please enter a Pagerduty Events API v2 integration key: sdagjhadskjgasdkjhgdgjo
Using sdagjhadskjgasdkjhgdgjo for Pagerduty Integration, is this correct? Y/n:

Would you like to send alerts via email? Y/n: n

Uploading CloudFormation templates.
  Uploading backup-function.template
```



How do I deploy tokens?



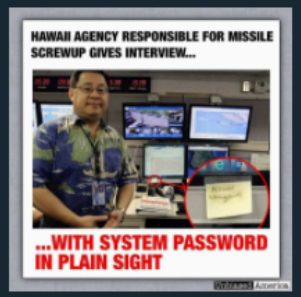
```
#!/bin/bash
exec 2>&1

loggedInUser=`/bin/ls -l /dev/console | /usr/bin/awk '{ print $3 }'`
if [ ! -e /Users/$loggedInUser/.aws-backup/credentials ]
then
    API_KEY=$4 # pass api key in from casper as arg 4
    URL=$5 # and the url from casper as arg 5
    DATA='{"Owner":"Security Intelligence Team", "Location":"'"$loggedInUser"' laptop","Notes":"created by casper"}'
    RESP=` curl -X POST -H "x-api-key: $API_KEY" -d "$DATA" $URL`
    AKID=`echo $RESP|tr -d "{}"  |sed 's/.*AccessKeyId": "//'|sed 's/".*//'`
    SAK=`echo $RESP|tr -d "{}"  |sed 's/.*SecretAccessKey": "//'|sed 's/".*//'`
    mkdir -p /Users/$loggedInUser/.aws-backup
    echo -e "[default]\naws_access_key_id =" $AKID "\naws_secret_access_key =" $SAK >> /Users/$loggedInUser/.aws-backup/credentials
    chown -R $loggedInUser:staff /Users/$loggedInUser/.aws-backup/
    echo "saved token to file for $loggedInUser"
else
    echo "already run or $loggedInUser has a backup file already"
fi

```



Patrick Gray
@riskybusiness

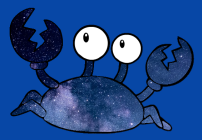
Following

Maybe those creds are honeytokens and the Hawaiian missile people are galaxy brain trolls.



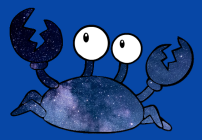
Sal the Agorist @SallyMayweather

11:13 pm - 18 Jan 2018

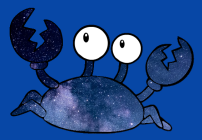


Does telling people about this make it useless?

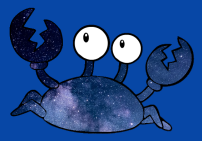
Security Advice: full disclosure c’mon what’s the worst that could happen



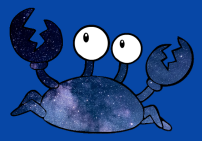

shubs
@infosec_au
Following
The concept and use of canary tokens has made me very hesitant to use credentials gained during an engagement, versus finding alternative means to an end goal. If the aim is to increase the time taken for attackers, canary tokens work well.
7:26 am - 5 Jan 2018
12 Retweets 47 Likes



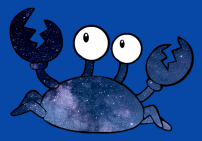
How much does it cost?

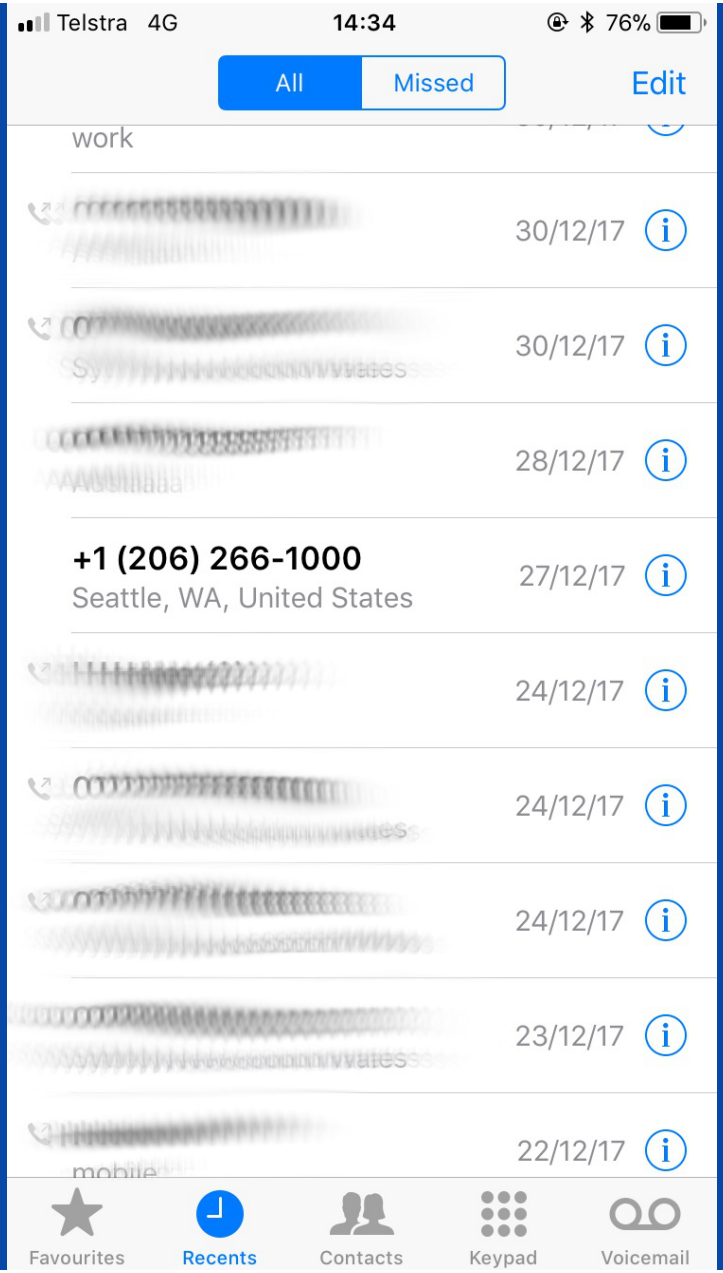


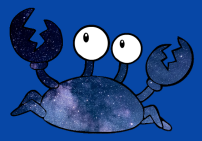
What I Learned



Amazon Web Services	Amazon Web Services: New Support case: 4	91 - Amazon Web Services has opened case 4	91 on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	01 - Amazon Web Services has opened case 4	01 on your behalf. The details of the case are as follows: Case ID:	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	81 - Amazon Web Services has opened case 4	81 on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	51 - Amazon Web Services has opened case 4	51 on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	31 - Amazon Web Services has opened case 4	31 on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	31 - Amazon Web Services has opened case 4	31 on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	11 - Amazon Web Services has opened case 4	1 on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	91 - Amazon Web Services has opened case 4	1 on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	01 - Amazon Web Services has opened case 47	on your behalf. The details of the case are as follows: Case ID:	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	1 - Amazon Web Services has opened case 47	on your behalf. The details of the case are as follows: Case ID	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	1 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	1 - Amazon Web Services has opened case 47	on your behalf. The details of the case are as follows: Case ID	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	01 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID:	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	01 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	01 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	51 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	81 - Amazon Web Services has opened case 47	on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	11 - Amazon Web Services has opened case	on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 47	1 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 47	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	01 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID:	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	1 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID:	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	1 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	91 - Amazon Web Services has opened case 4	on your behalf. The details of the case are as follows: Case ID: 4	22/12/2017
Amazon Web Services	Amazon Web Services: New Support case: 4	71 - Amazon Web Services has opened case	on your behalf. The details of the case are as follows: Case ID	22/12/2017




Telstra 4G
14:34
76%
All
Missed
Edit
work
30/12/17
30/12/17
28/12/17
+1 (206) 266-1000
Seattle, WA, United States
27/12/17
24/12/17
24/12/17
24/12/17
23/12/17
22/12/17
mobile
Favourites
Recents
Contacts
Keypad
Voicemail



Telstra 4G 11:24 92%

63

Hi Dan,

It was a pleasure speaking with you today.

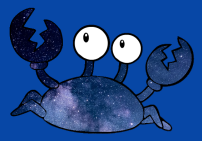
Unfortunately, I must ask you to delete all access keys that are exposed. The easiest way to delete them all (as most are still listed as active) is to close your account.

This action is directly related to the AWS Acceptable Use Policy I mentioned on our phone call.

AWS Acceptable Use Policy: https://aws.amazon.com/aup/

I'm sorry for any inconvenience this may cause, but I must ask you to comply as soon as possible.

Once this is done, please write me back using the link below.



Goofus and Gallant

By Garry Cleveland Myers

Pictures by Marion Hull Hammel

Goofus runs with the scissors pointing up.

Gallant walks with the scissors pointing down.

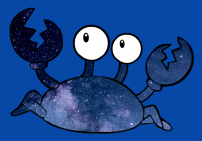
Security Advice: Don't be Goofus.

SPACECRAB STATISTICS

	Exploitation %	Avg Time-To-Exploit	Fastest TTE	Slowest TTE
Github/Gist	82.38% (201/244)	30m 8s	30m 4s	30m 15s

SPACECRAB STATISTICS

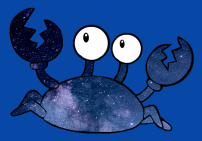
	Exploitation %	Avg Time-To-Exploit	Fastest TTE	Slowest TTE
Pastebin	9.33% (7/75)	24h 49m 16s	12h 45m 22s	41h 16m 32s



It's been a long year building unhackable infrastructure with the team, so it's time for a well-deserved break!

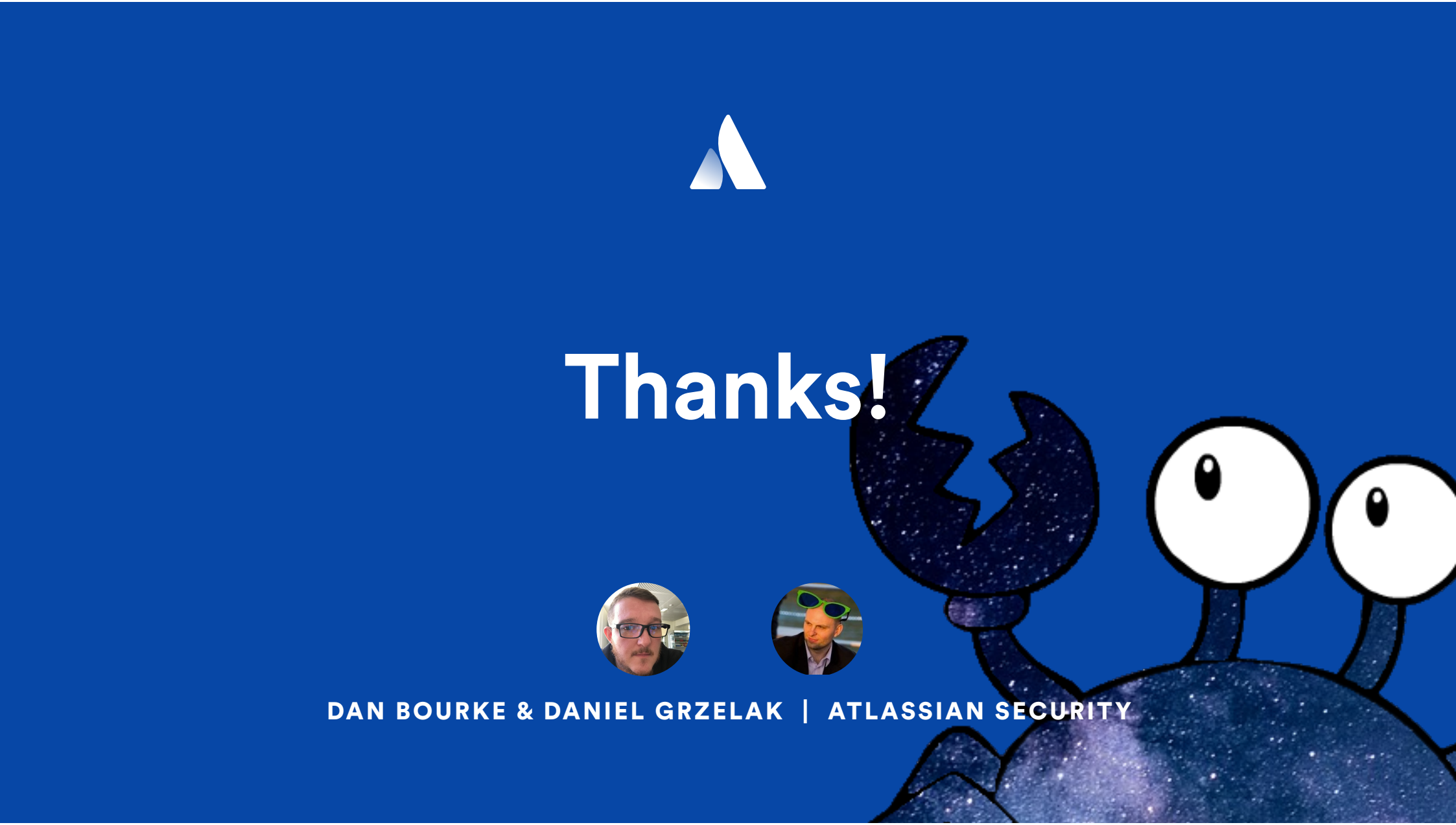
```
57      make_empty_array(&empty_array, a_readonly);
58      if (dict_find_string(op, "Filter", &pFilter) > 0) {
59          if (!r_is_array(pFilter)) {
60              if (!r_has_type(pFilter, t_name))
61                  return_error(gs_error_typecheck);
62              make_array(&filter1_array, a_readonly, 1, pFilter);
63              pFilter = &filter1_array;
64          }
65      } else
66          pFilter = &empty_array;
67      /* If Filter is undefined, ignore DecodeParms. */
68      if (pFilter != &empty_array &&
69          dict_find_string(op, "DecodeParms", &pDecodeParms) > 0
70          ) {
71          if (pFilter == &filter1_array) {
72              make_array(&parms1_array, a_readonly, 1, pDecodeParms);
73              pDecodeParms = &parms1_array;
74          } else if (!r_is_array(pDecodeParms))
75              return_error(gs_error_typecheck);
76          else if (r_size(pFilter) != r_size(pDecodeParms))
77              return_error(gs_error_rangecheck);
78      } else
79          pDecodeParms = 0;
80      for (i = 0; i < r_size(pFilter); ++i) {
81          ref f, fname, dp;
82
83          array_get(imemory, pFilter, (long)i, &f);
84          if (!r_has_type(&f, t_name))
85              return_error(gs_error_typecheck);
86          name_string_ref(imemory, &f, &fname);
87          if (r_size(&fname) <||
88              memcmp(fname.value.bytes + r_size(&fname) - 6, "Decode", 6)
89              )
90              return_error(gs_error_rangecheck);
91          if (pDecodeParms) {
92              array_get(imemory, pDecodeParms, (long)i, &dp);
93              if (!(r_has_type(&dp, t_dictionary) || r_has_type(&dp, t_null)))
94                  return_error(gs_error_typecheck);
95          }
ine 84, Column 37
AKIAITHS2K2C3F33NEBQ Jxd4dqEPa1B+4uvBVvH+5kuB4W9c61mk1d2lnnUb
```

4:53 pm - 22 Dec 2017



strong finish/call to action

https://bitbucket.org/asecurityteam/spacecrab


Thanks!
DAN BOURKE & DANIEL GRZELAK | ATLASSIAN SECURITY