#FIRSTCON24

Collaboratively Caring & Securely Sharing of Information That Matters

Dr Dave Matthews, Gen Digital (Avast/NortonLifelock), AU

Whoami @work

> 25 years in Cyber: Engineering, Forensics and IR

Australian National University

System Administrator - Phd in Statistics

Worked – Government, Corporate, Defense, Law Enforcement, then

CROWDSTRIKE Avast Gen

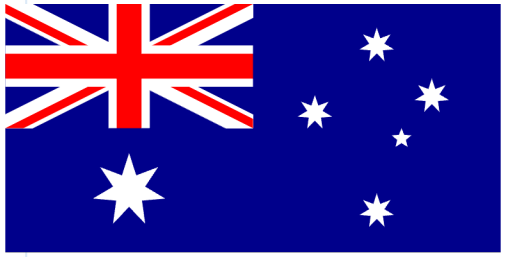
From Brisbane, Australia

FIRST Improving Security Together

Went to my first, 'FIRST' conference in 1999!

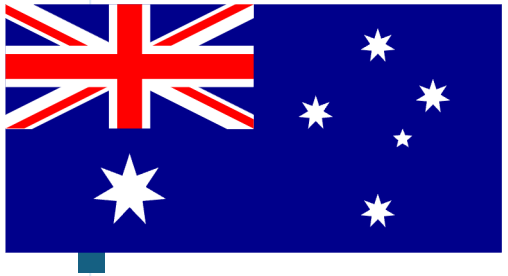
Contact and Slides at end of talk

#FUNinJapan



Welcome
To
Australia!

#FUNinOz!

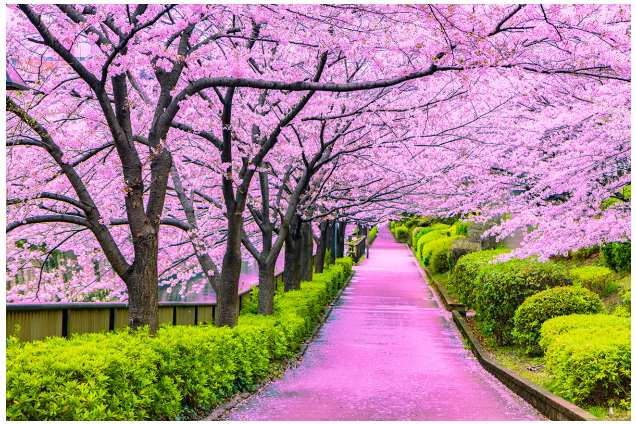


#FUNinOz!

Talk Outline

- Sharing Intel – it can help you, and others
- When might we want to share?
- What is stopping us?
- Describe a way to make this easy
- Hopefully this can help all of us..

Intel Sharing is Valueable



- FIRST's mission:

"to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large."

- Theme of #FIRSTCON24:

BRIDGING SECURITY RESPONSE GAPS

Lack of Sharing - Widely Recognised as an Issue

ASD sees "frequency, richness" of cyber info sharing fall away

By Ry Crozier

Feb 14 2024 6:35AM

Reinforces the need to set up new trusted info exchange mechanisms.

The Australian Signals Directorate has lamented a decline in the "frequency and richness" of cyber incident data shared with it by the private sector, underlining – it says – the importance of restoring trusted channels for information exchange.

Lack of Sharing - Widely Recognized as an Issue

Sharing Communities: The Good, the Bad, and the Ugly

Thomas Geras*
HM Munich University of Applied Sciences
Munich, Germany
thomas.geras@hm.edu

Thomas Schreck*
HM Munich University of Applied Sciences
Munich, Germany
thomas.schreck@hm.edu

between security teams was necessary. One problem was that no explicit team was responsible for coordinating the measures against the attack, but many organizations connected to the Internet had their own security team. That led to the creation of the first sharing community called the "Forum of Incident Response and Security Teams" (FIRST) [10].

(https://dl.acm.org/doi/10.1145/3576915.3623144 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security)

Sharing Intel Rapidly – what's stopping us?

Sharing intel might be difficult due to person's role or workplace

It's hard – what's the best way to share – anonymously?

Some people are reluctant – for fear of being criticized!

Scenario 1: your company is breached because of a 3rd party compromise

- Example: Breach occurred from your use of the MOVEit managed file transfer software
- Your Incident Response revealed artifacts that could be used to identify compromise
- How to share these to help others?
- Without revealing that your organization has been breached??

Scenario 2: your Intelligence detects likely compromised Organisation

- Eg. Darkweb monitoring indicates that a company - *may* be compromised – Threat Actor auctioning access
- Initial Access Brokers (IAB) do this to sell to eCrime groups
- Essential to alert the compromised company fast… before ransomware operators move in to achieve their mission….
- You believe you have identified the compromised company

Scenario 2: your Intel detects likely compromised Company

exploit[.]in [redacted]

ACCESS: Domain Admins. Enterprise Admins.

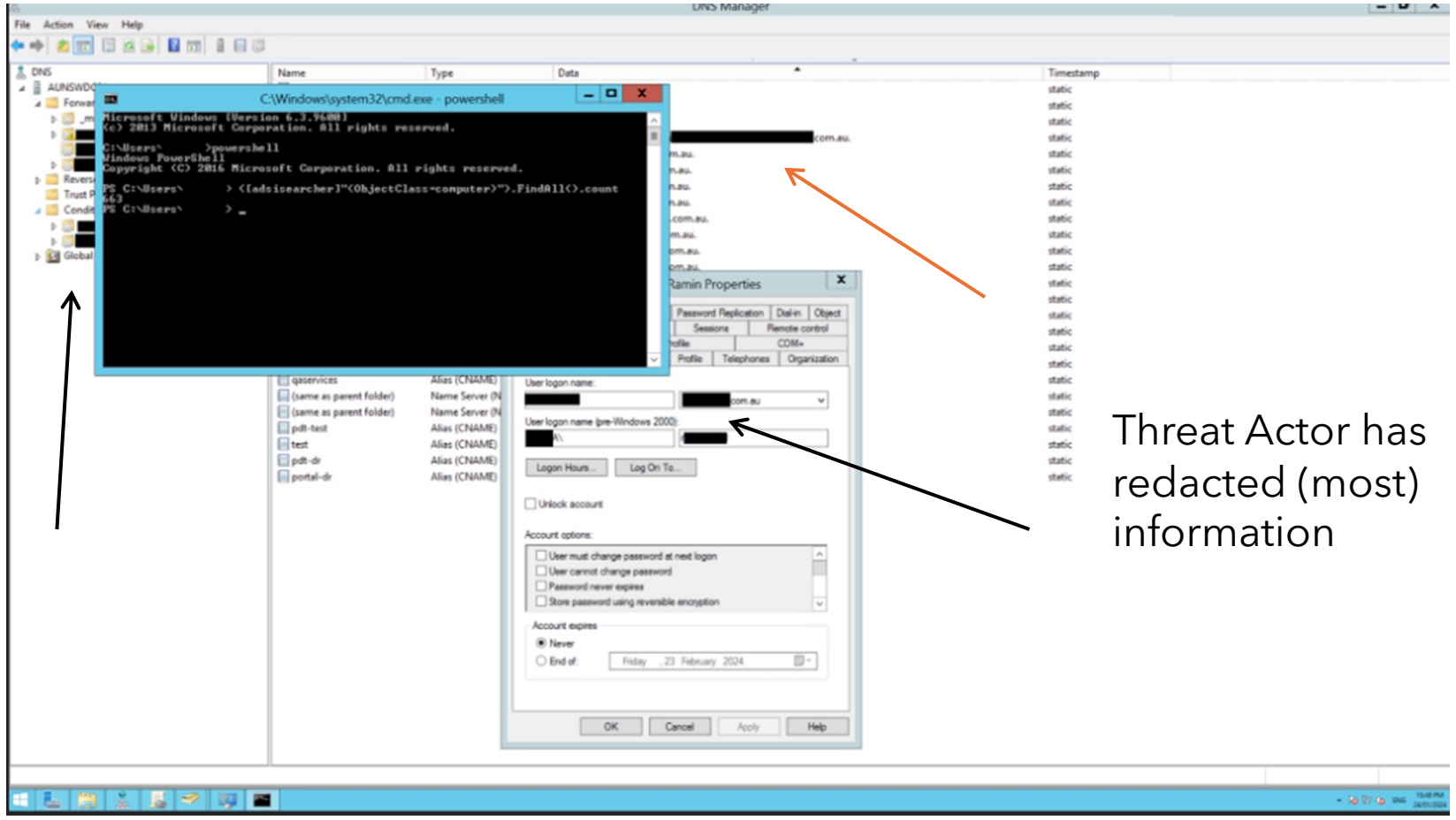
Country: [redacted]
Industry:Freight & Logistics Services. Transportation (By Zoominfo)

A market leader in Records and Information Management (RIM)
revenue:$91 Million
4 DC
1350 Users
663 PC
+ldap dump
+Files with all architecture and servers
+KDBX file with all passwords for all servers(but don't know pass from kdbx)
AV: Symantec Endpoint Protection (You can disable it. Without password)

Start 1500$
step 500$
Blitz 10000$

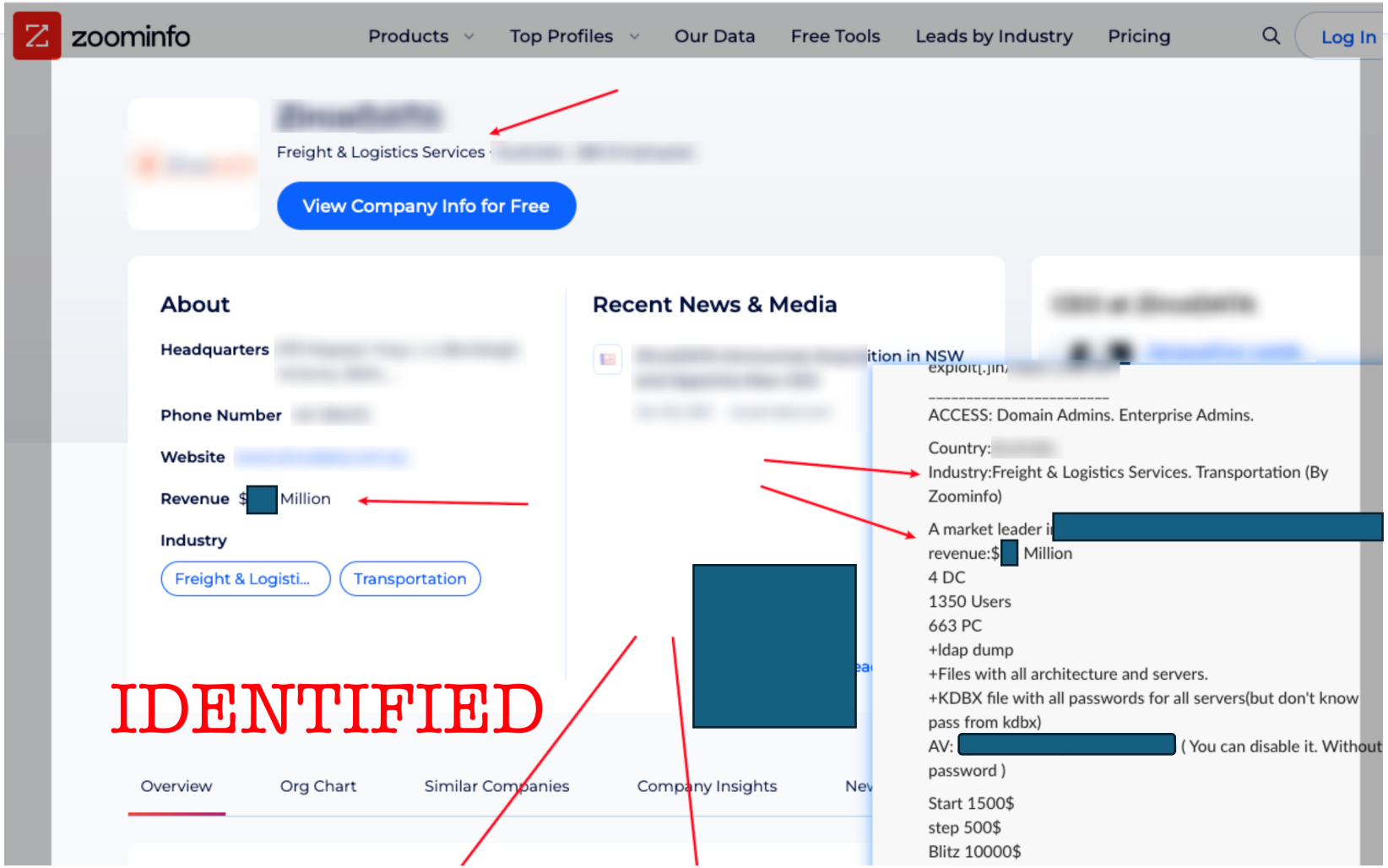
BREACH FORUM

Scenario 2: your Intel detects likely compromised Company



Threat Actor has redacted (most) information

Scenario 2: your Intel detects likely compromised Company – You Identified Them!



Scenario 3: critical vuln in VPN product – many vulnerable instances found on internet

- Eg. A VPN vendor has another CVSS 10.0 bug released
- You scan your attack surface to check your footprint
- Shodan/Censys scanning shows many exposed hosts
- You would like to alert the owners of these hosts
- It’s the right thing to do – but how?

Scenario 4: you have found details in dark web leak

- Eg. As result of investigation into a case, you have found data in threat actor's leak site – eg. Acme Corp
- Want to share this information with the Acme Corp cyber team – completely anonymously

Scenario 5: You Have Been Hacked – you Need Help

- Eg. Your company has been ransomed – you have some samples of what you believe are the encryptors and other IOC's
- How can you share them?
- Because sharing them, as yourself, will indicate to others that your company has been breached..

Questions for Audience

- Who has been involved in an incident response case?
- Do any of these scenarios sound familiar?
- Did you wish that you could anonymously share lessons or info you learned about the case?

Hopefully, have explained the problem

- These scenarios highlight the problem of sharing without revealing your identity.
- Let’s talk about a possible solution….

Introducing

Secret Squirrel

https://en.wikipedia.org/wiki/Secret_Squirrel

Secret Squirrels – a mythical and fictional Sharing Community

Background:

- The Secret Squirrels are an association of Cyber Security professionals
- They use a Slack Workspace to communicate and share information
- Membership is only by invitation – you have to be vetted/introduced by someone else already in the Secret Squirrels Community

- A lot of Sharing Communities work like this
- (NOTE: nothing special about Slack – this can also be done for Teams/Discord/Mattermost)

Secret Squirrel Intel Sharing

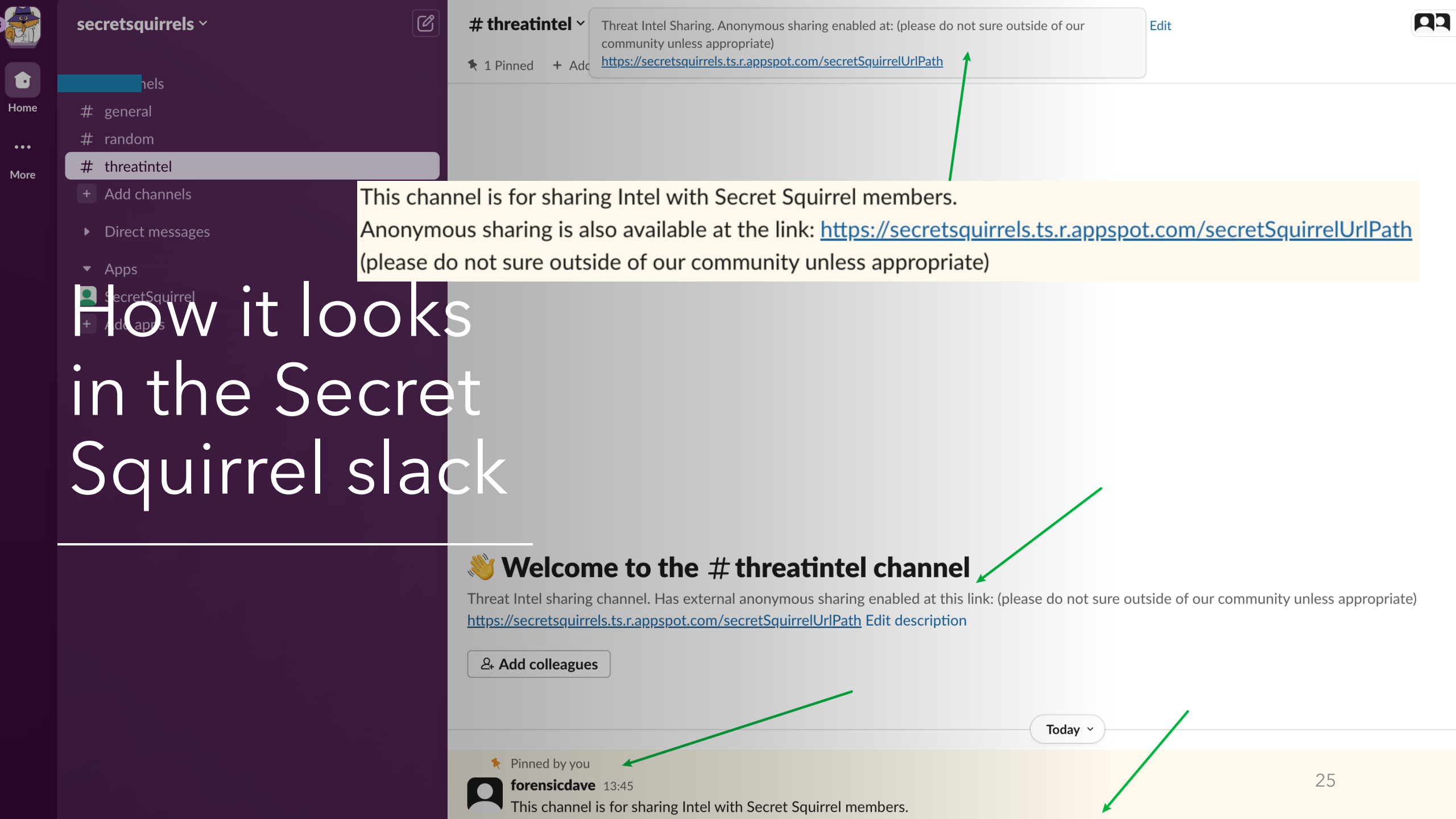
- Secret Squirrel Slack workspace has a channel dedicated to sharing useful threat intelligence - #threatintel
- Usually, information is shared here from Open Source
- Other times members might share early released information not yet published…
- We show how you can add the ability to post information anonymously to #threatintel

#threatintel channel

- This channel has a pinned message:

"To publish intel anonymously – go to this Website"

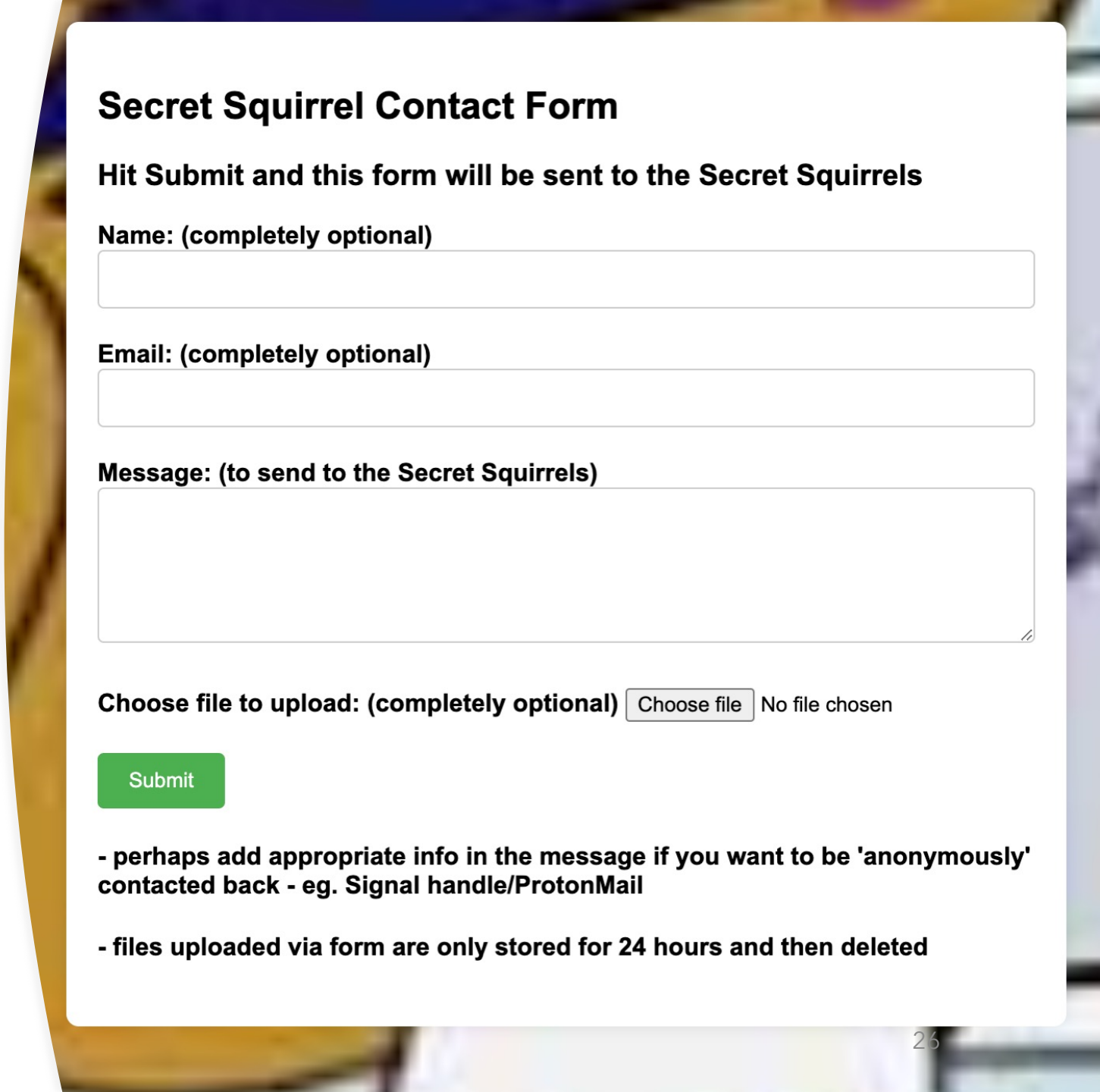
- The Website hosts a Form with fields for:
  - Name: (optional)
  - Email address: (optional)
  - Message field: The Text that you want to share.
- When the form is filled out, and Submitted
  it Posts a new message to the #threatintel channel


secretsquirrels
Home
More
general
random
threatintel
Add channels
Direct messages
Apps
SecretSquirrel
threatintel
1 Pinned
Threat Intel Sharing. Anonymous sharing enabled at: (please do not sure outside of our community unless appropriate)
https://secretsquirrels.ts.r.appspot.com/secretSquirrelUrlPath
Edit
This channel is for sharing Intel with Secret Squirrel members.
Anonymous sharing is also available at the link: https://secretsquirrels.ts.r.appspot.com/secretSquirrelUrlPath
(please do not sure outside of our community unless appropriate)
How it looks in the Secret Squirrel slack
Welcome to the # threatintel channel
Threat Intel sharing channel. Has external anonymous sharing enabled at this link: (please do not sure outside of our community unless appropriate)
https://secretsquirrels.ts.r.appspot.com/secretSquirrelUrlPath Edit description
Add colleagues
Today
Pinned by you
forensicdave 13:45
This channel is for sharing Intel with Secret Squirrel members.

Web site for anonymous submission

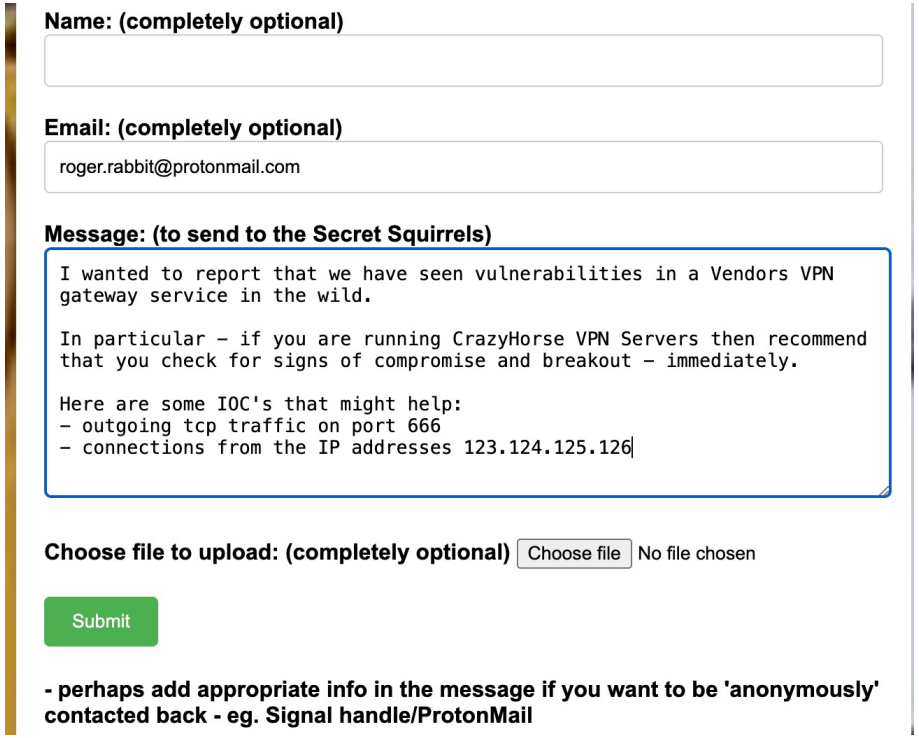
- Hosted on a ‘hidden’ URL
- Can be password protected
- Optionally supply name / email /message
- Even upload a file

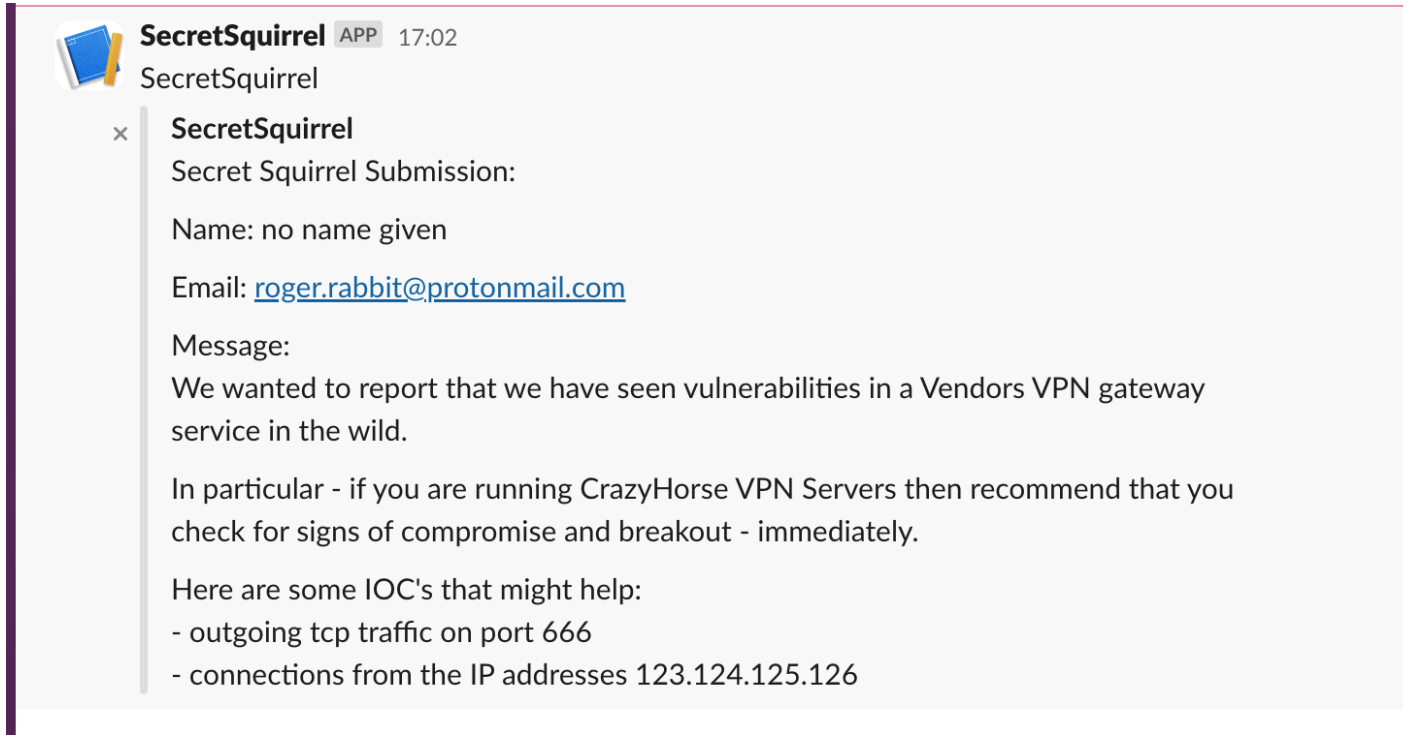
- Clicking submit sends a message to Slack/Teams/Discord/Mattermost channel



Example:

- Anonymous submission of Threat Intel to channel





Let’s Revisit the earlier Scenarios

- We’ll show some examples of how you could use this service

Scenario 1: your company is breached because of 3rd party compromise

- Example: Breach occurred from your use of the MOVEit managed file transfer software
- Your Incident Response revealed artifacts that could be used to identify compromise
- How to share these to help others?
- Without revealing that your organization has been breached??

Scenario from use

Secret Squirrel Contact Form

Hit Submit and this form will be sent to the Secret Squirrels

Name: (completely optional)

Email: (completely optional)

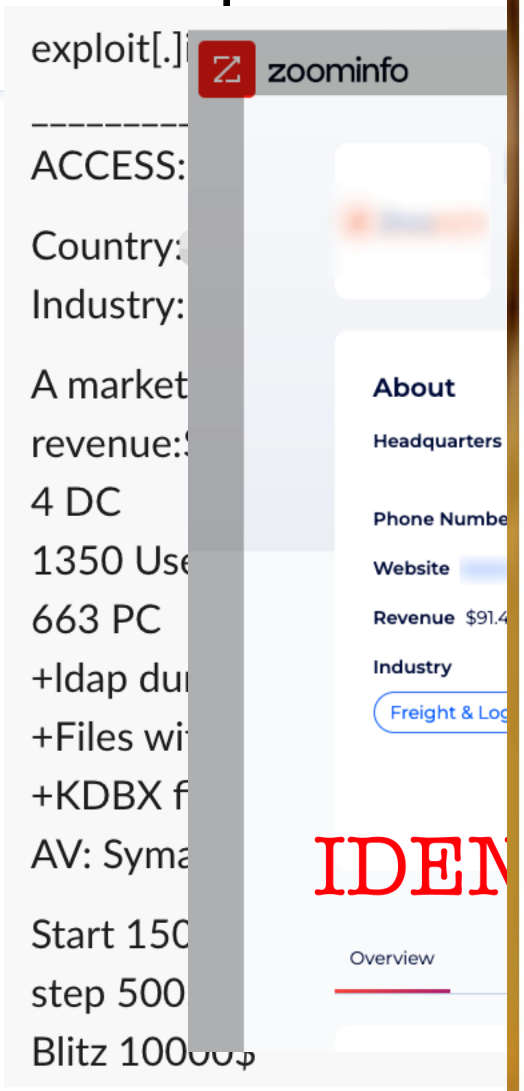
Message: (to send to the Secret Squirrels)

```
Hi. We run MOVEit File transfer software.
Unfortunately for us, we have been compromised.

Here are some ways of determining if you too have been compromised,
and how to identify what was exfiltrated:

......


If you have any queries feel free to ping back on Signal
on my handle 'KingJulien' or i_like_to_moveit_moveit@protonmail.com
```

Choose file to upload: (completely optional) Choose file No file chosen

Submit

Scenario 2: compromis



Name: (completely optional)

Email: (completely optional)

Message: (to send to the Secret Squirrels)

```
Hi. Our intel picked up a Breach Forum notice about IAB claiming to
have gained a foothold into a company.

After looking at some of their screenshots we believe that this
company is the ACME Heavy Industries CORP.

Have attached an encrypted zip (password is 'squirrel') which
contains screenshots and our analysis.

If anyone has a contact at ACME Heavy Industries CORP please alert
them.
```

Choose file to upload: (completely optional) Choose file ACMECORP.zip

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously' contacted back - eg. Signal handle/ProtonMail

- files uploaded via form are only stored for 24 hours and then deleted

y

Scenario

- Eg. Your co
  - Unusual
  - strange
- How can yc
- Asking dire
  may have b
- So, Ask Anc

Secret Squirrel Contact Form

Hit Submit and this form will be sent to the Secret Squirrels

Name: (completely optional)

Email: (completely optional)

solarwindsurfer@protonmail.com

Message: (to send to the Secret Squirrels)

```
Hi there. We use SolarWinds to monitor our network.

Our monitoring of DNS traffic has detected regular external
DNS queries to multiple random looking Domain Names from
Solarwinds processes in our network.

Our EDR has not flagged anything as suspicious (yet) - would
like to share this to see if any of you have seen the same.

Have attached a encrypted zip file with a PCAP of the DNS
traffic
```

Choose file to upload: (completely optional) Choose file SOLARWINDS.zip

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously' contacted back - eg. Signal handle/ProtonMail

- files uploaded via form are only stored for 24 hours and then deleted

Scena ...eed help

- Eg. Yo... ...have some sample... ...rs and other IOC's
- How c...
- Sharin... ...company has been b...
- So, ask...

Hit Submit and this form will be sent to the Secret Squirrels

Name: (completely optional)

DESPERATE DAVE

Email: (completely optional)

HELP_US_PLEASE@protonmail.com

Message: (to send to the Secret Squirrels)

```
HELP!!

Unfortunately we have just suffered a massive ransomware
event!!

All of our Domain Controllers and many workstations are
encrypted.

We have invoked our IR retainer but they cannot attend for
another day and have to travel to us by plane.

Have included a zip with the ransomware note and the encryptor
that we recovered from a memory dump (it was deleted).

Any help with attribution or ANYTHING would be greatly
appreciated!!!

Please email on Proton or contact on Signal at DESPERATE_DAVE
```

Choose file to upload: (completely optional) Choose file ARTIFACTS.zip

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously'

Scena

- Unfortu
- The ‘Cu
- Anonyr

Name: (completely optional)

Email: (completely optional)

Message: (to send to the Secret Squirrels)

```
Hi, I'm seeking help.

We have seen some large data transfers from our network to
addresses that resolve to the MEGA.IO domain.

Does this sound like something we should worry about?
```

Choose file to upload: (completely optional) Choose file No file chosen

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously' contacted back - eg. Signal handle/ProtonMail

- files uploaded via form are only stored for 24 hours and then deleted

Scenario 4: Ju

- Sometimes, you ju
- Without fear of re
  "That has already
  "That's old news"
  etc

Secret Squirrel Contact Form

THRUNTING_REPORT2024.pdf

Hit Submit and this form will be sent to the Secret Squirrels

Name: (completely optional)

Email: (completely optional)

Message: (to send to the Secret Squirrels)

```
Here is a copy of the latest Annual Threat Report
from Threat Hunters Intel Team.

To save you signing up with your details, I did :-)

Have attached a VirusTotal Scanned PDF for your enjoyment!
```

Choose file to upload: (completely optional) Choose file THRUNTING2024.pdf

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously' contacted back - eg. Signal handle/ProtonMail

- files uploaded via form are only stored for 24 hours and then deleted

Sharing information – bidirectionally

- Sharing information one way is (mostly) straightforward
- How to share both ways – ie. how to communicate back to the anonymous poster?
- In our SS #threatintel example - potentially they might Direct Message
- An alternative – when sharing info – the Anonymous poster could provide a Signal Handle/Anon email address for Out-Of-Band communication
- It depends…. On the Sharing Community .. And What Works for You..

One Key Benefit of this - It Encourages Sharing

- Some users will prefer to post anonymously:
- Less fear of criticism
- Or repercussions
- In a vetted Sharing Community this could work well

How to set it up - yourself

- High level overview
  - Setup Incoming Webhook in your Slack/Teams/Discord channel
  - Configure webserver front end and host it on internet (or Tor)
  - Webserver has web form – takes inputs from user
    - Can be obscure URL
    - Or password protected
  - When user submits data to web form, data is parsed and sent to Webhook in your messaging platform
  - Users who are in the WebHook enabled channel will see the message

Implementation - Overview

- Configure a Google Compute Cloud instance
  - (New customers also get $300 in free credits to run, test, and deploy)
- Run Python Flask webserver in Google App Engine
- Can provide example code as template/guide
  - Change code to use your webhook
  - Create your version of the web form
- Costs very little to run
- Very little to no maintenance

Implementation – Google Cloud

- Chose Google Cloud to host webserver
  - simple, economical and easy – sample code shortly in my Github repo
- Steps are detailed there – but an overview:
- 1. Create new GCP Project
- 2. Create python Google App engine and upload Python Flask Web app
  - Application has web server configuration for different URL paths
  - Configured with webhooks used to send data to Instant Messaging Platform
- 3. Configure Google Storage Bucket for files uploaded to Web app
  - Set Lifecycle for storage to auto delete after required period (24h in my eg)

Python Webserver Configuration Overview

- Configure Webhook(s) in your messaging platform
- Create html frontend template for your desired look/feel
- Configure Python Webserver with mappings to webhook(s):
-

```
@app.route('/secretSquirrelUrlPath', methods=['GET', 'POST'])
def secretSquirrel():
        # CODE to handle requests goes here
        # if GET then return web form
        # if POST then handle web form input and send to WEBHOOK
        #   with unique link to storage location for any uploads
#end def secretSquirrel()
```

Web Frontend supports multiple webhooks

- Handlers with unique URL paths can be configured
  - Can host multiple different front-end pages or Urls
  - each can be associated with different webhooks
  - Eg. One for #threatintel another for #anonymousFeedback or #helpneeded
- And – this works with webhooks go to almost any messaging platform Slack/Teams/Discord/Mattermost

Webhooks don’t support uploading files – how we solved

- You might want to offer ability to upload files to your channel
- File upload could be screenshots/suspected malware/zip and could of course be encrypted by user before uploading.
- We Solve This by implementing file upload option in web form
- The Python Flask webserver uploads files to a Google Cloud Storage Bucket and returns a ‘hidden’ link to the file
- Eg. https://storage.googleapis.com/.../6a933c3d-3ac6-4d0d-969b-aae81e9b1ffe/684f3af1-7aba-4183-ab0a-507f37c8e00d/47744832-28cc-4eb8-a860-f8622c4cf07a

File upload – how it looks to user

SecretSquirrel APP 20:39

SecretSquirrel

> **SecretSquirrel**
> Secret Squirrel Submission:
>
> Name: no name given
>
> Email: no email given
>
> Message:
> Here is a copy of the latest Annual Threat Report
> from Threat Hunters Intel Team.
>
> To save you signing up with your details, I did :-)
>
> Have attached a VirusTotal Scanned PDF for your enjoyment!
>
> File Upload:
> The file 'THRUNTING2024.pdf' was uploaded..
> This File is available at this link for 24 hours:
> https://storage.googleapis.com/secretsquirrels.appspot.com/f4d64b6c-8074-48d5-87f2-0f425e6c7fe4/3d642430-97d9-48e0-b026-47d07933be32/3cd5772e-2f8a-4ec6-982d-cf07651242d2.pdf

Potential Issues

- Really Need Good instructions on how to use this
- People could upload but say they are other people
- Consider the sensitivity of information being shared
- This system might be best implemented in a vetted information sharing environment where everyone has a common mission

What about automation?

- Wrote some simple command line tooling
  - It enables sending messages to the webhook destination - *via* the front-end website
  - Webhook is kept ‘secret’ – sends via the same URL used by users
  - Might be useful for automating sending of anonymous Intel to the messaging workspace

Example ‘api’ usage: ‘squirrelApi’

- For fun – call this the squirrelApi:

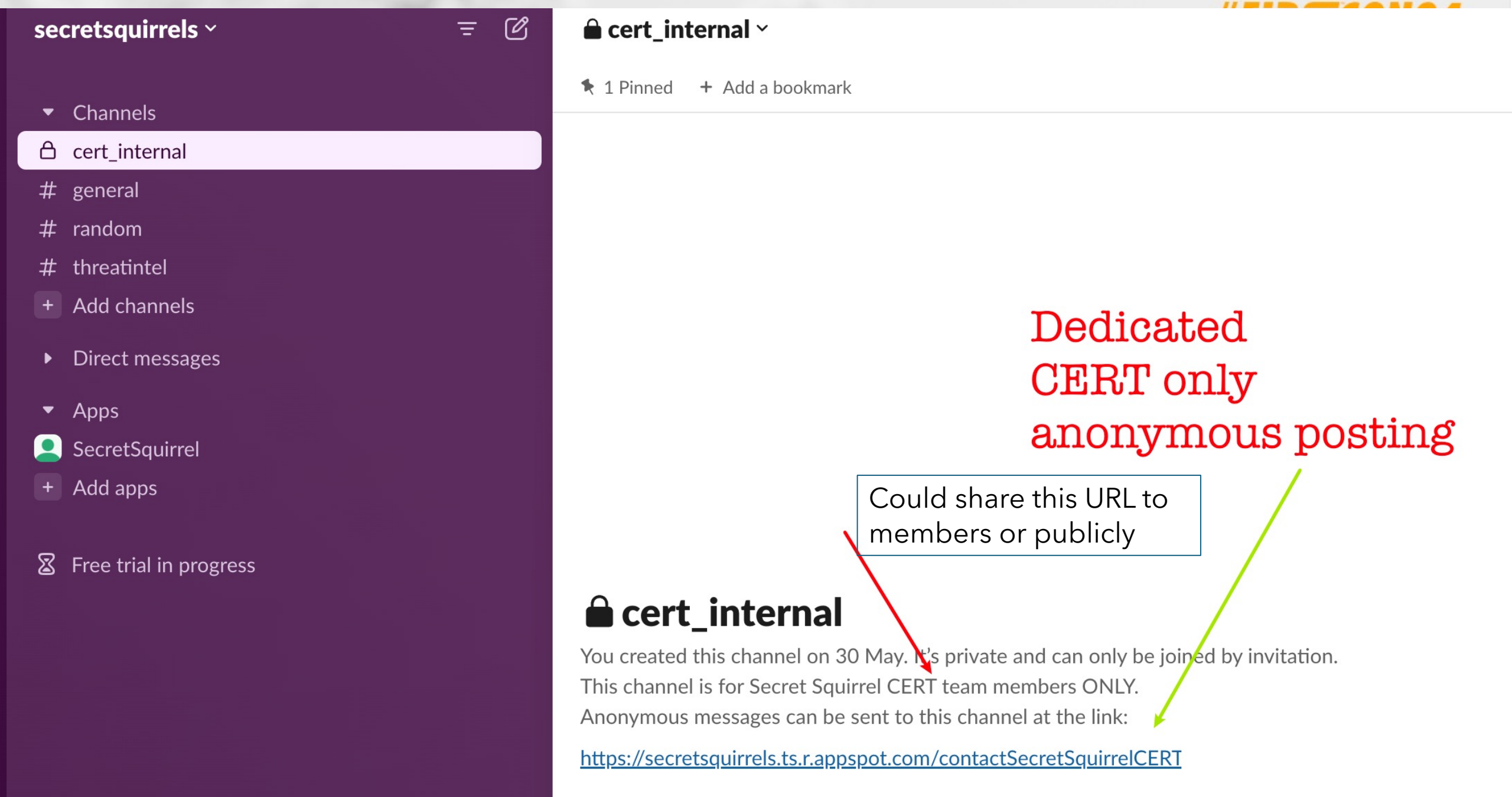
```
usage: squirrelApi.py [-h] [--filename FILENAME] [--name NAME] [--email EMAIL] --message MESSAGE

Secret Squirrel Message Sender

options:
  -h, --help            show this help message and exit
  --filename FILENAME   Set to the path to the filename
  --name NAME           Your name - if you want to give one!
  --email EMAIL         Your email address - if you want to give one!
  --message MESSAGE     The message you want to send

Examples:
squirrelApi.py --filename="pathToFile" --message "here is something important i want you to know"
```

- Script is configured with the special website location and username/password (if required)
- Could be used to automate feed of information into channel

Many Other Use Cases

#CERTonly – channel for CERT members only

- Eg. Anon ‘tip-offs’ to your CERT team
- Used for Emergency Incident Response team members only
- Hosted via a Different URL / webhook


secretsquirrels
Channels
cert_internal
general
random
threatintel
Add channels
Direct messages
Apps
SecretSquirrel
Add apps
Free trial in progress
cert_internal
1 Pinned
Add a bookmark
Dedicated CERT only anonymous posting
Could share this URL to members or publicly
cert_internal
You created this channel on 30 May. It's private and can only be joined by invitation.
This channel is for Secret Squirrel CERT team members ONLY.
Anonymous messages can be sent to this channel at the link:
https://secretsquirrels.ts.r.appspot.com/contactSecretSquirrelCERT

Secret Squirrel CERT Contact Form

Hit Submit and this form will be sent to the Secret Squirrels CERT Team - noone else

Name: (completely optional)

Email: (completely optional)

Message: (to send to the Secret Squirrels CERT Team)

Choose file to upload: (completely optional) Choose file No file chosen

Submit

- perhaps add appropriate info in the message if you want to be 'anonymously' contacted back - eg. Signal handle/ProtonMail

#FIRSTCON24

Secret Squirrel CERT Contact Form

Hit Submit and this form will be sent to the Secret Squirrels CERT Team - noone else

Name: (completely optional)

Email: (completely optional)

Message: (to send to the Secret Squirrels CERT Team)

```
Dear CERT team,

We have received Intelligence that indicates that the
Big ACME Corporation - perhaps one of your member organisations -
has been compromised by threat actors.

It is hosting malicious content on their web servers.

We have attached a zip file containing screenshots and other related
evidence. The password is 'i like nuts'

If you wish to contact us back then you can do so on the email
alvinTheChipmunk@protomail.com

Many thanks
```

Choose file to upload: (completely optional) Choose file evidence.zip

Submit

#FIRSTCON24

福

36TH ANNUAL
FIRST CONFERENCE
FUKUOKA
JUNE 9-14, 2024 JAPAN

secretsquirrels

Home
DMs
Activity
More

Channels
cert_internal
general
random
threatintel
Add channels

Direct messages

Apps
CERTonly
SecretSquirrel
Add apps

Free trial in progress

cert_internal

1 Pinned + Add a bookmark

Today

CERTonly APP 21:54
SecretSquirrel

SecretSquirrel
Secret Squirrel CERT Submission:

Name: no name given

Email: no email given

Message:
Dear CERT team,

We have received Intelligence that indicates that the
Big ACME Corporation - perhaps one of your member organisations -
has been compromised by threat actors.

It is hosting malicious content on their web servers.

We have attached a zip file containing screenshots and other related evidence. The password is 'i like nuts'

If you wish to contact us back then you can do so on the email
alvinTheChipmunk@protomail.com

Many thanks

File Upload:
The file 'evidence.zip' was uploaded..
This File is available at this link for 24 hours:
https://storage.googleapis.com/secretsquirrels.appspot.com/49bb8694-055b-424d-b5f5-77a37d954214/e4f7a1e1-8d9c-48e8-98d2-a35bf356597e/60827e5c-822c-

Other use cases

Not just limited to #intel ….

- ‘anonymous’ comms can be used in lots of situations
- As with everything – there can be downsides so needs good planning..

Summary

- Talk was about a way of sharing information in a ‘secret-like’ manner
- Flexible, and straightforward to implement
- Way of enabling sharing of information ‘anonymously’ that could help with Incident Response and Intel Sharing

Thank you!!

- Why not - Set up your own Secret Sharing System
- QR code has link to my contact details
- Any questions? Please contact me:

https://linkedin.com/in/drdavematthews

dave.matthews

- Sample code is going up at github.com/forensicdave
- Can give you access to the Secret Squirrels Slack to try out – if you like! DM me ☺