OK Google, How do I Red Team GSuite?

Attacking Google Suite Customers

Mike Felch & Beau Bullock

Who We Are

- Mike Felch - @ustayready
  - Pentest / Red team at BHIS
  - Involved w/ OWASP Orlando & BSides Orlando
  - Host of Tradecraft Security Weekly
  - Host of CoinSec Podcast
- Beau Bullock - @dafthack
  - Pentest / Red team at BHIS
  - Host of Tradecraft Security Weekly
  - Host of CoinSec Podcast
  - Avid OWA enthusiast

Relationship Status

Disclaimer: ~~We <3 Google~~

We broke up :(It's complicated...

What We’re Covering

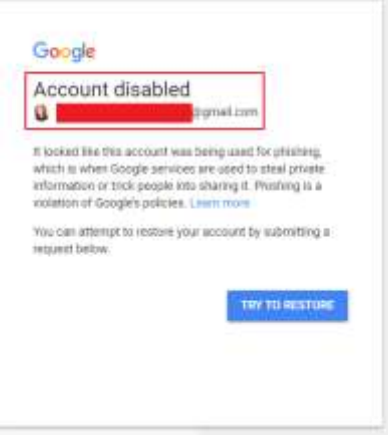
1. Preparation: OPSEC or Die Trying
2. External: Crack the Perimeter
3. SE: Exploiting Trust
4. Persistence: Hide in Plain Sight
5. Internal: Collateral Damage
6. Demo: Real-world Attack
7. Defending: Triage the Breach
8. *Questions / Comments*

Preparation:
OPSEC or Die Trying

Preparation: Bad! :(

How To Lose a Fight With Google SOC

- Use your normal account for API keys
- Login to multiple accounts w/ the same IP
- Use the same browser w/ multiple sessions

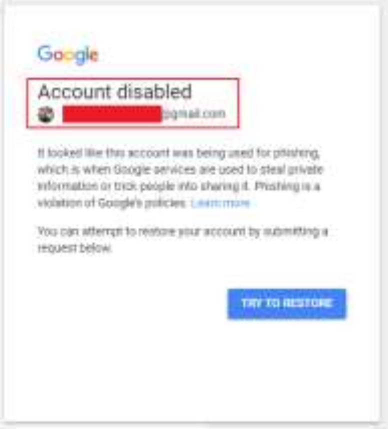


Account disabled

[redacted]@gmail.com

It looked like this account was being used for phishing, which is when Google services are used to steal private information or trick people into sharing it. Phishing is a violation of Google's policies. Learn more

You can attempt to restore your account by submitting a request below.

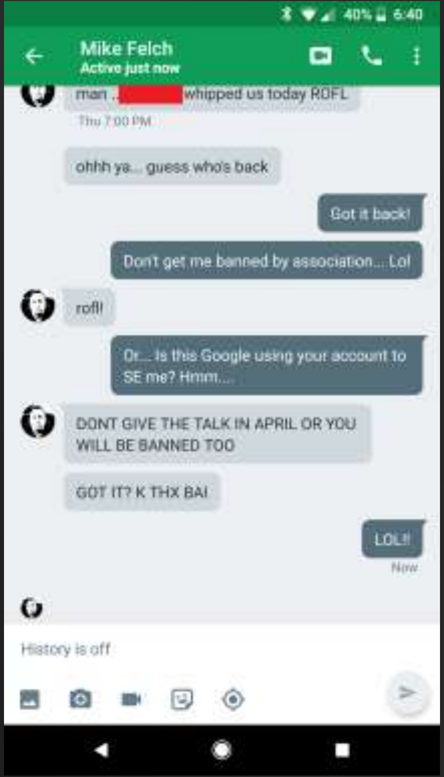


Account disabled

[redacted]@gmail.com

It looked like this account was being used for phishing, which is when Google services are used to steal private information or trick people into sharing it. Phishing is a violation of Google's policies. Learn more

You can attempt to restore your account by submitting a request below.



Mike Felch
Active just now

man .[redacted] whipped us today ROFL

Thu 7:00 PM

ohhh ya... guess who's back

Got it back!

Don't get me banned by association... Lol

rofl!

Or... Is this Google using your account to SE me? Hmm...

DONT GIVE THE TALK IN APRIL OR YOU WILL BE BANNED TOO

GOT IT? K THX BAI

LOL!!

Now

History is off

Preparation: Good! :)

+

+

$20-$500
OneVanilla
Prepaid Mastercard
Use every day for – online shopping, pay bills, travel, & more!
NO FEES
After Purchase

Preparation

- Prepaid Smartphone ✓
- Prepaid Credit Card ✓
- VPN Account ✓
- Clean Virtual Machine ✓
- New Google Identity ✓
- New Google API Keys ✓
- Don’t Cross-contaminate ✓

External:
Crack the Perimeter

Don’t move so quick!

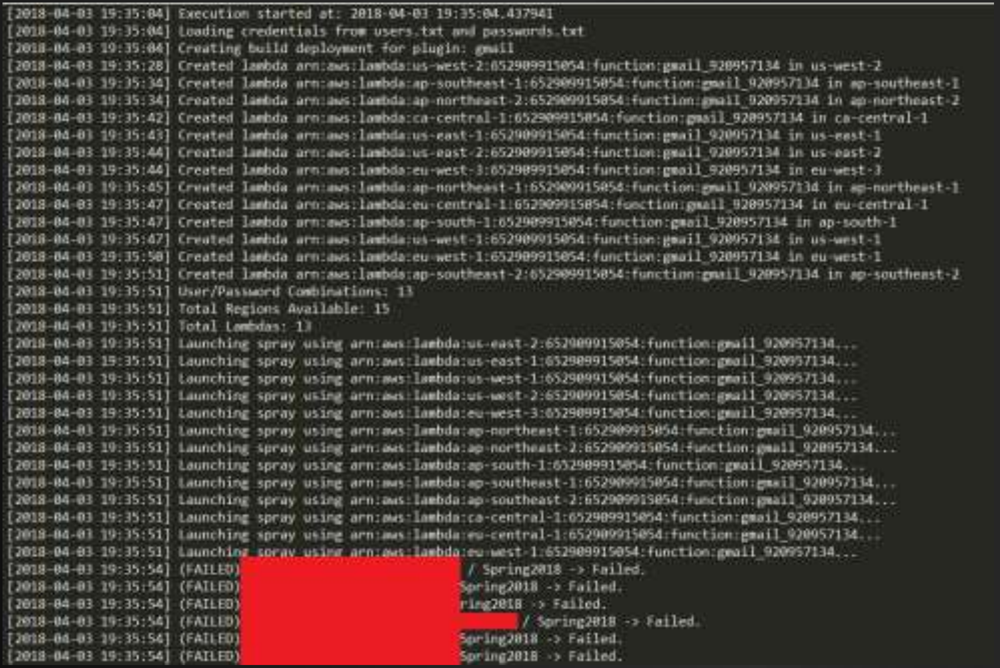
- Don’t go straight to shell
- Phishing w/ malicious docs are old
- Why go External -> Internal -> External???
- Decide on an attack path
- Strategically target victims

Creds are King!

SO FOR OUR FIRST DATE, I WAS THINKING WE COULD
FIGURE OUT NAMES FOR OUR CHILDREN

Password Spraying

- Determine naming convention
- Search LinkedIn for users
- Generate email lists
- Try one password at a time
- Spray all the accounts
- Rotate IP addresses regularly
- Just need one account to start



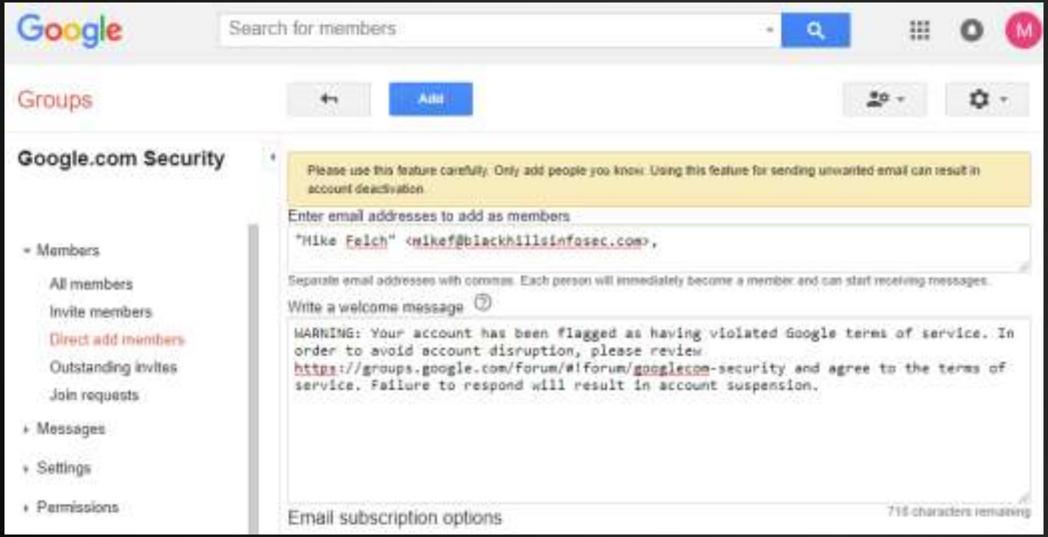
```
[2018-04-03 19:35:04] Execution started at: 2018-04-03 19:35:04.437941
[2018-04-03 19:35:04] Loading credentials from users.txt and passwords.txt
[2018-04-03 19:35:04] Creating build deployment for plugin: gmail
[2018-04-03 19:35:28] Created lambda arn:aws:lambda:us-west-2:652909915054:function:gmail_920957134 in us-west-2
[2018-04-03 19:35:34] Created lambda arn:aws:lambda:ap-southeast-1:652909915054:function:gmail_920957134 in ap-southeast-1
[2018-04-03 19:35:34] Created lambda arn:aws:lambda:ap-northeast-2:652909915054:function:gmail_920957134 in ap-northeast-2
[2018-04-03 19:35:42] Created lambda arn:aws:lambda:ca-central-1:652909915054:function:gmail_920957134 in ca-central-1
[2018-04-03 19:35:43] Created lambda arn:aws:lambda:us-east-1:652909915054:function:gmail_920957134 in us-east-1
[2018-04-03 19:35:44] Created lambda arn:aws:lambda:us-east-2:652909915054:function:gmail_920957134 in us-east-2
[2018-04-03 19:35:44] Created lambda arn:aws:lambda:eu-west-3:652909915054:function:gmail_920957134 in eu-west-3
[2018-04-03 19:35:45] Created lambda arn:aws:lambda:ap-northeast-1:652909915054:function:gmail_920957134 in ap-northeast-1
[2018-04-03 19:35:47] Created lambda arn:aws:lambda:eu-central-1:652909915054:function:gmail_920957134 in eu-central-1
[2018-04-03 19:35:47] Created lambda arn:aws:lambda:ap-south-1:652909915054:function:gmail_920957134 in ap-south-1
[2018-04-03 19:35:47] Created lambda arn:aws:lambda:us-west-1:652909915054:function:gmail_920957134 in us-west-1
[2018-04-03 19:35:50] Created lambda arn:aws:lambda:eu-west-1:652909915054:function:gmail_920957134 in eu-west-1
[2018-04-03 19:35:51] Created lambda arn:aws:lambda:ap-southeast-2:652909915054:function:gmail_920957134 in ap-southeast-2
[2018-04-03 19:35:51] User/Password Combinations: 13
[2018-04-03 19:35:51] Total Regions Available: 15
[2018-04-03 19:35:51] Total Lambdas: 13
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:us-east-2:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:us-east-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:us-west-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:us-west-2:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:eu-west-3:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ap-northeast-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ap-northeast-2:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ap-south-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ap-southeast-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ap-southeast-2:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:ca-central-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:eu-central-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:51] Launching spray using arn:aws:lambda:eu-west-1:652909915054:function:gmail_920957134...
[2018-04-03 19:35:54] (FAILED)[redacted] / Spring2018 -> Failed.
[2018-04-03 19:35:54] (FAILED)[redacted]pring2018 -> Failed.
[2018-04-03 19:35:54] (FAILED)[redacted]ring2018 -> Failed.
[2018-04-03 19:35:54] (FAILED)[redacted] / Spring2018 -> Failed.
[2018-04-03 19:35:54] (FAILED)[redacted]Spring2018 -> Failed.
[2018-04-03 19:35:54] (FAILED)[redacted]Spring2018 -> Failed.
```

Demo:
AWS Lambda Spraying

SE:
Exploiting Trust

Google Group Ruse

- Create malicious group
- Change your display name
- Force add users
- Customize a message
- Don’t forget URLs...



Please use this feature carefully. Only add people you know. Using this feature for sending unwanted email can result in account deactivation

Enter email addresses to add as members

"Mike Felch" <mikef@blackhillsinfosec.com>,

Separate email addresses with commas. Each person will immediately become a member and can start receiving messages.

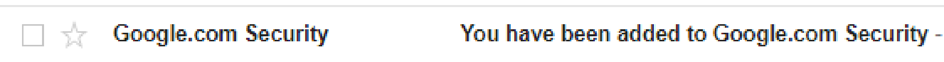
Write a welcome message

WARNING: Your account has been flagged as having violated Google terms of service. In order to avoid account disruption, please review https://groups.google.com/forum/#!forum/googlecom-security and agree to the terms of service. Failure to respond will result in account suspension.

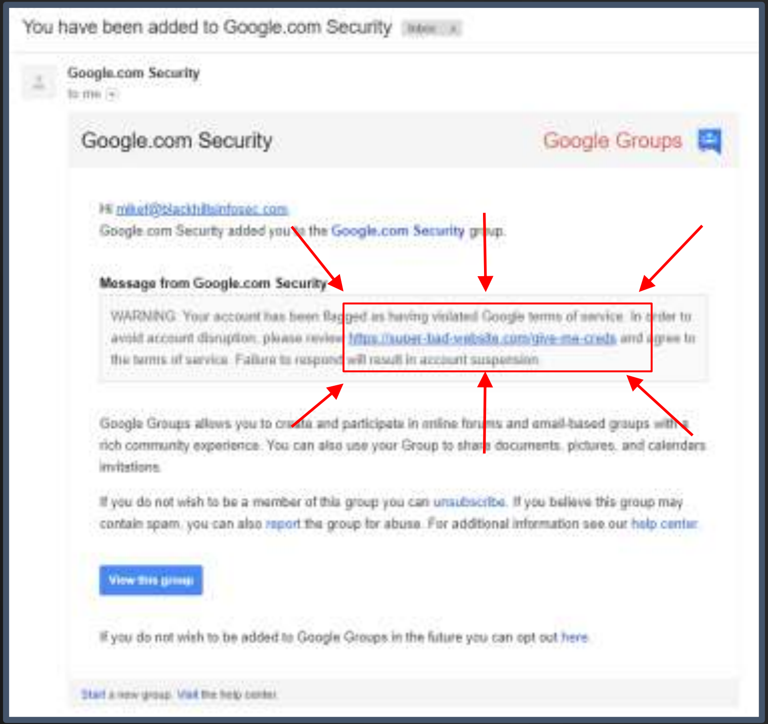
716 characters remaining

Email subscription options

Google Group Ruse



□ ☆ Google.com Security You have been added to Google.com Security -



You have been added to Google.com Security Inbox x

Google.com Security
to me

Google.com Security Google Groups

Hi mikef@blackhillsinfosec.com
Google.com Security added you to the Google.com Security group.

Message from Google.com Security

WARNING: Your account has been flagged as having violated Google terms of service. In order to avoid account disruption, please review https://super-bad-website.com/give-me-creds and agree to the terms of service. Failure to respond will result in account suspension.

Google Groups allows you to create and participate in online forums and email-based groups with a rich community experience. You can also use your Group to share documents, pictures, and calendars invitations.

If you do not wish to be a member of this group you can unsubscribe. If you believe this group may contain spam, you can also report the group for abuse. For additional information see our help center.

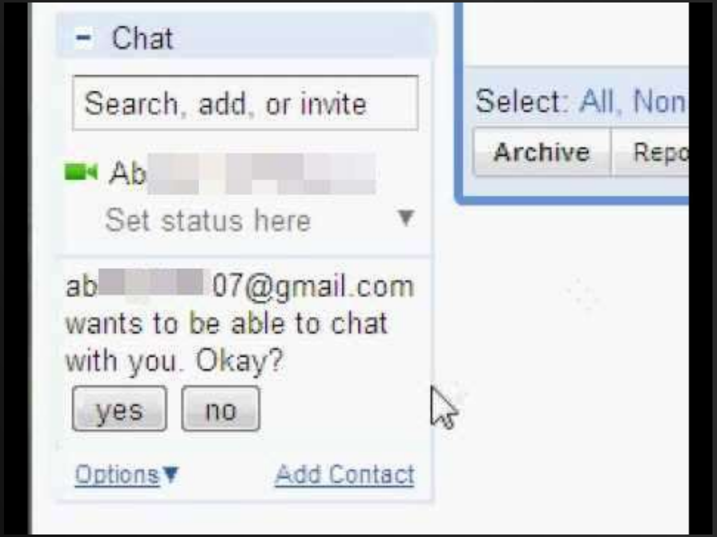
View this group

If you do not wish to be added to Google Groups in the future you can opt out here.

Start a new group. Visit the help center.

Google Hangout Ruse

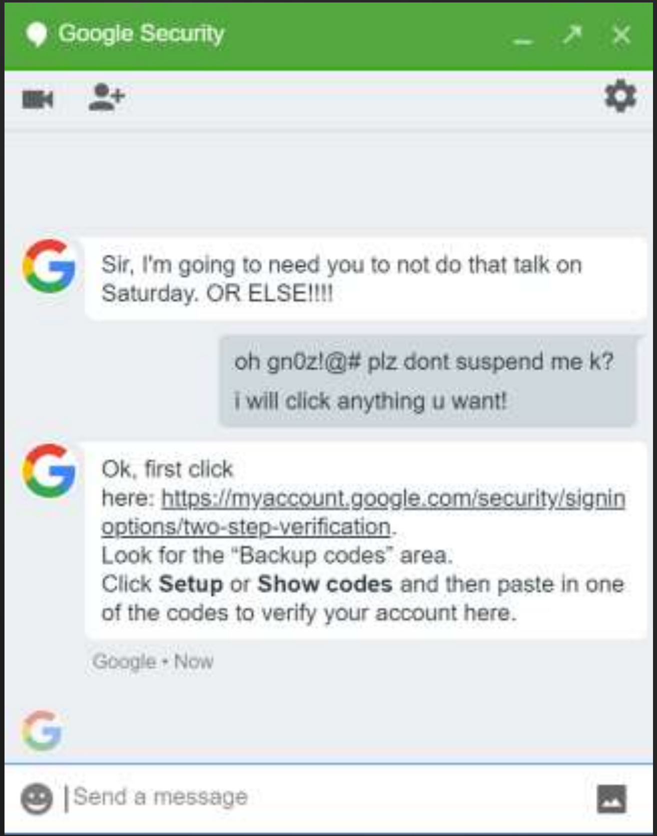
- Remember this? ----------->
- This was an invite to chat in Gmail
- Apparently this was too much work for some users



ab[redacted]07@gmail.com wants to be able to chat with you. Okay?

Google Hangout Ruse

- Now the default Google Hangouts settings allow direct chat without warning
- Simply knowing the email address is all that’s needed
- Pop a message box open to the target spoofing another person
- Say hi, send link, capture creds and/or shell



Sir, I'm going to need you to not do that talk on Saturday. OR ELSE!!!!

oh gn0z!@# plz dont suspend me k?

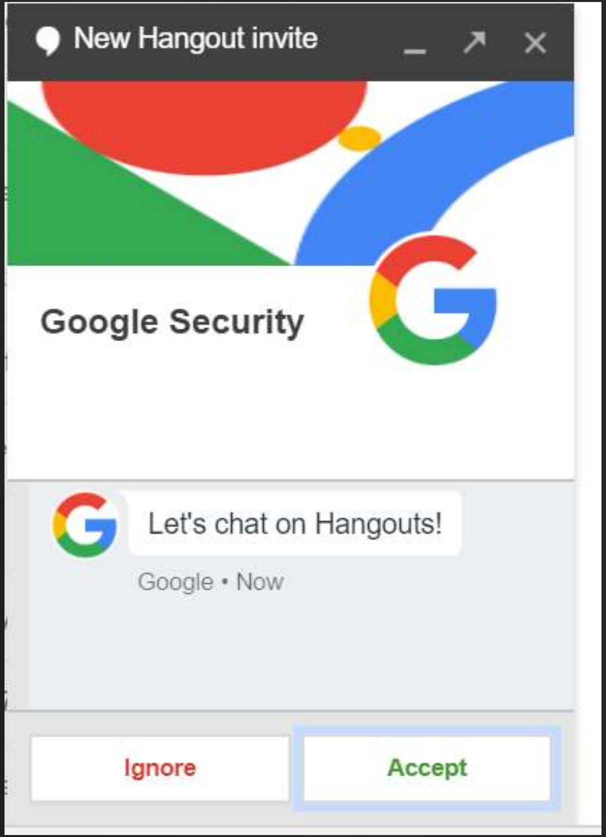
i will click anything u want!

Ok, first click here: https://myaccount.google.com/security/signinoptions/two-step-verification.
Look for the "Backup codes" area.
Click **Setup** or **Show codes** and then paste in one of the codes to verify your account here.

Google • Now

Google Hangout Ruse

- You can modify your default settings to enforce sending an invitation
- But even then, spoofed accounts look good
- To require invites:
  - Hangouts.google.com, click hamburger menu in top left, Settings, “Customize Invite Settings”, switch all to “Can send you an invitation”
- There doesn’t appear to be a global option for locking down accounts across an org



New Hangout invite

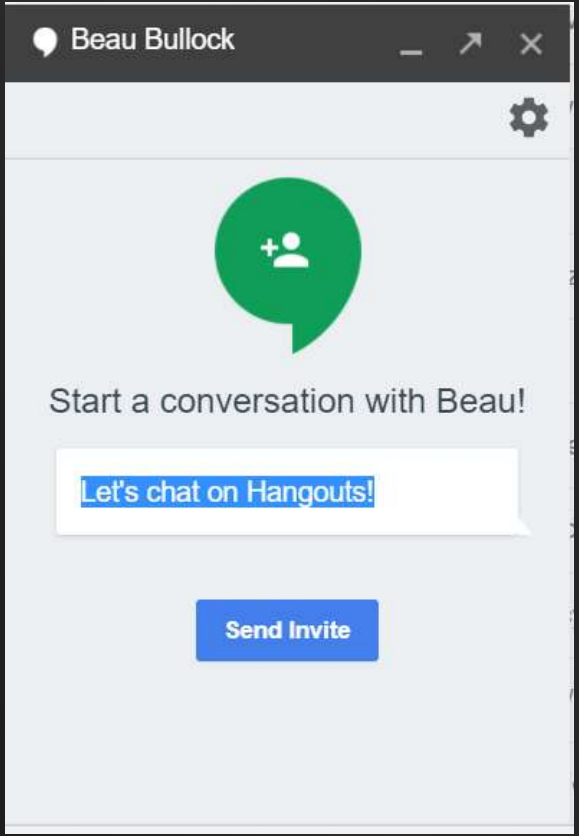
Google Security

Let's chat on Hangouts!

Google • Now

Enumerate Open Accounts

- Accounts not requiring invites can be enumerated easily
- Simply start a new chat with them via the Gmail chat menu
- If the box that pops up says “Start a conversation with <name>” then an invite is required



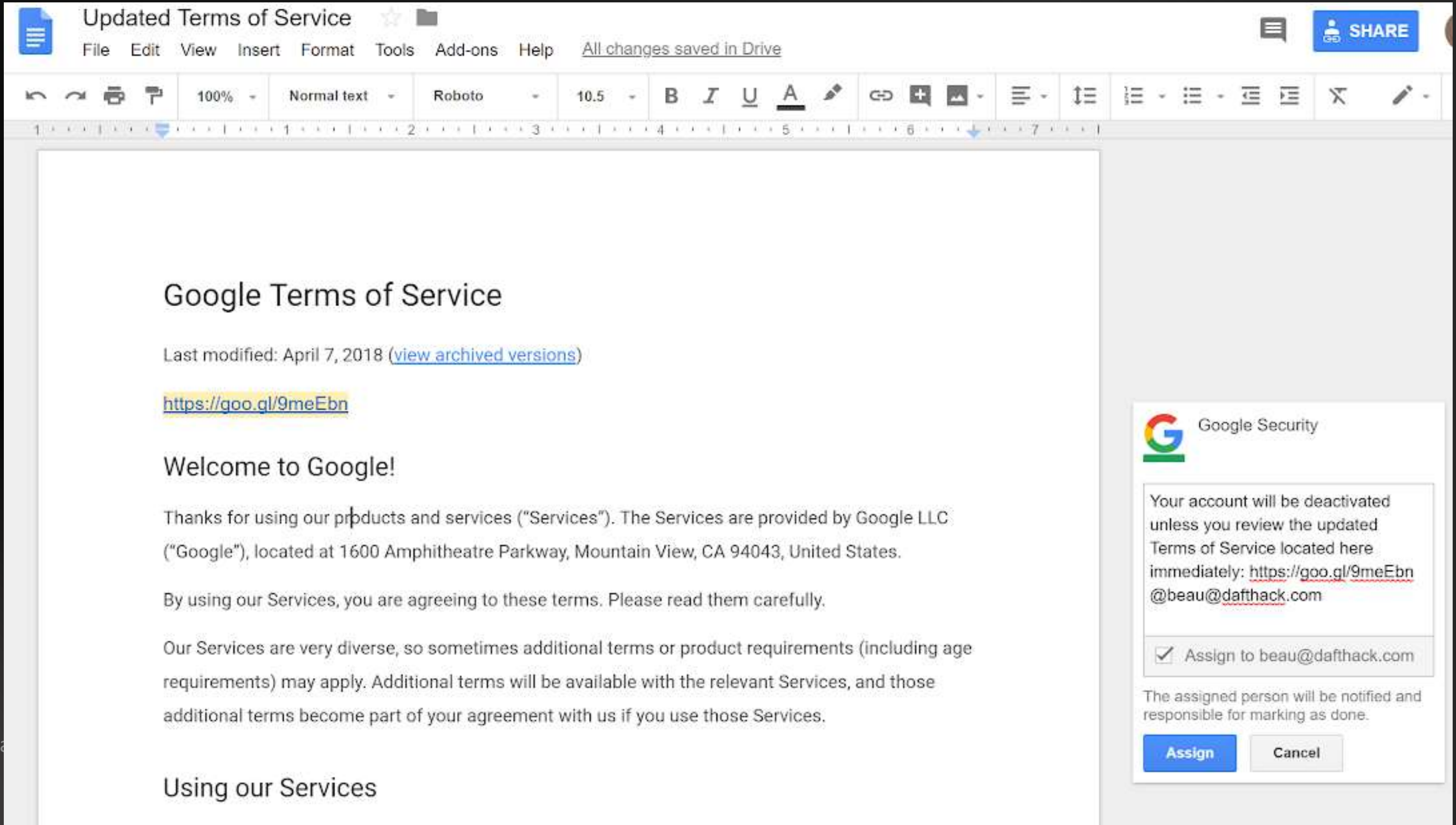
Start a conversation with Beau!

Let's chat on Hangouts!

Google Doc Ruse

- What if you could get Google to send a phishing link for you?
- Google Docs is perfect for this
  - Create a Google Doc with clickbait name like "Critical Update Pending"
  - Add content, then add a comment to the doc with your phishing link
  - In the comment, type their email address prefixed with a + symbol *(i.e. +hacker@gmail.com)* then check 'Assign'
  - Google will send the target an email from <random-string>@docs.google.com

Google Doc Ruse



Google Terms of Service

Last modified: April 7, 2018 (view archived versions)

https://goo.gl/9meEbn

Welcome to Google!

Thanks for using our products and services ("Services"). The Services are provided by Google LLC ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

Using our Services

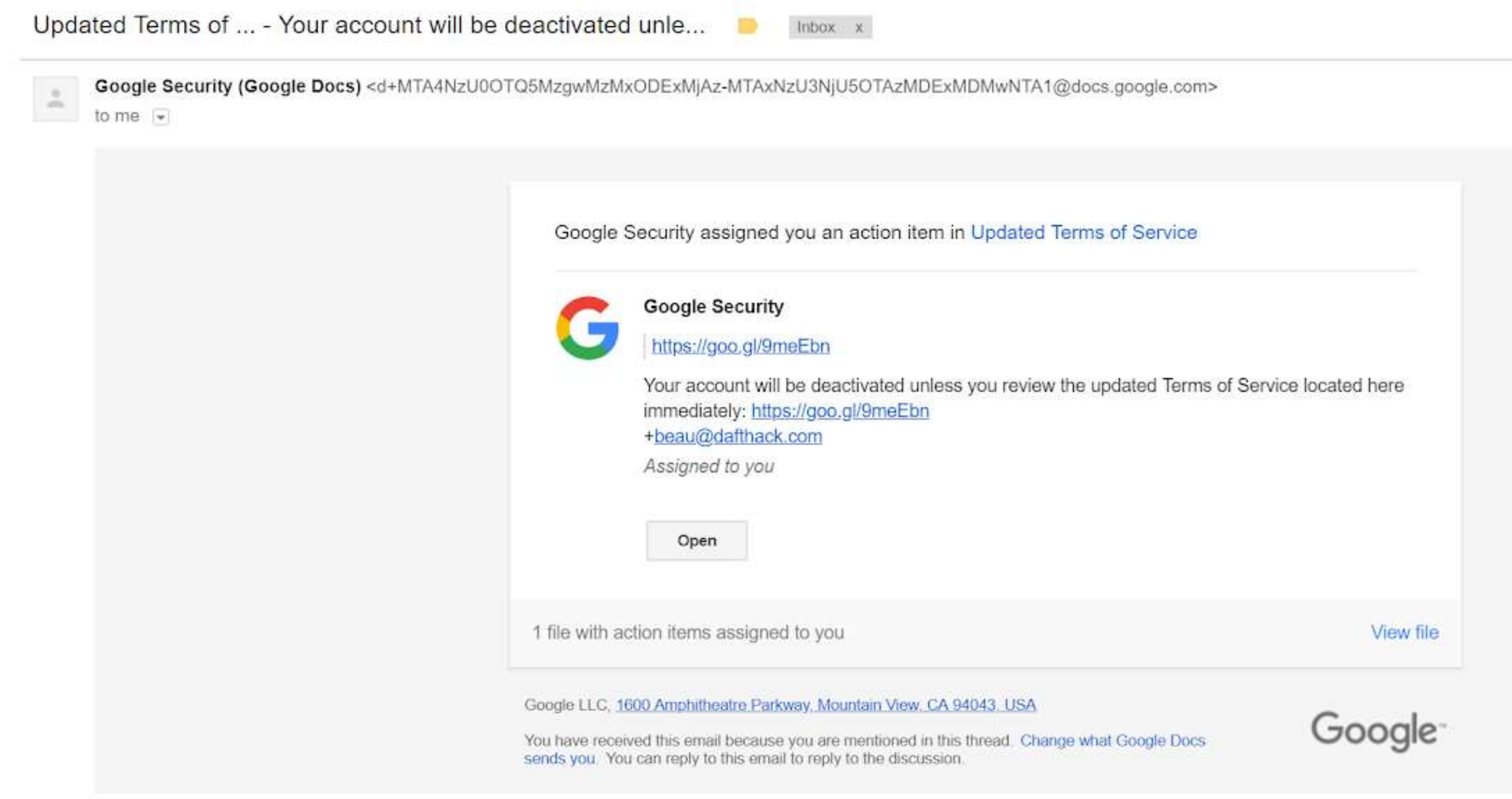
Google Security

Your account will be deactivated unless you review the updated Terms of Service located here immediately: https://goo.gl/9meEbn @beau@dafthack.com

☑ Assign to beau@dafthack.com

The assigned person will be notified and responsible for marking as done.

Google Doc Ruse



Updated Terms of ... - Your account will be deactivated unle...

Google Security (Google Docs) <d+MTA4NzU0OTQ5MzgwMzMxODExMjAz-MTAxNzU3NjU5OTAzMDExMDMwNTA1@docs.google.com>
to me

Google Security assigned you an action item in Updated Terms of Service

Google Security

https://goo.gl/9meEbn

Your account will be deactivated unless you review the updated Terms of Service located here immediately: https://goo.gl/9meEbn
+beau@dafthack.com

Assigned to you

1 file with action items assigned to you

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

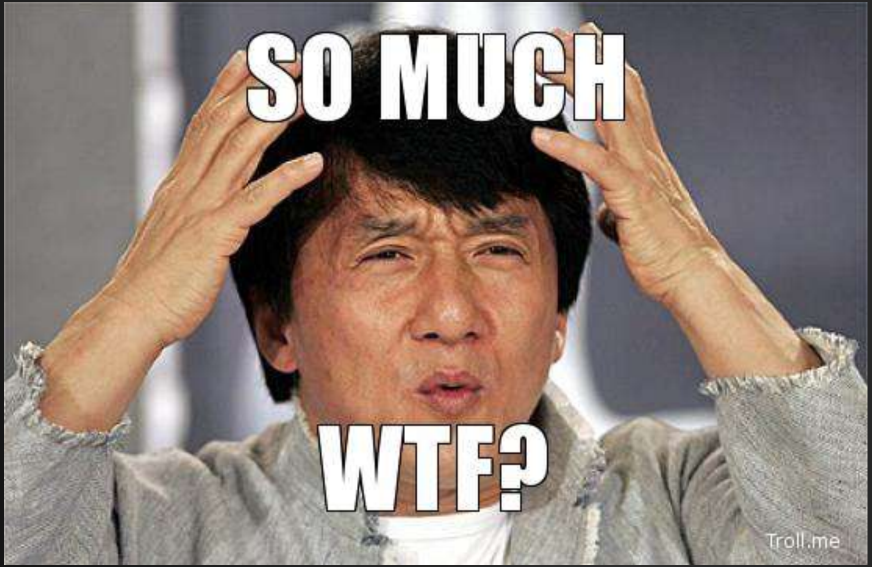
You have received this email because you are mentioned in this thread. Change what Google Docs sends you. You can reply to this email to reply to the discussion.

Google

Google Calendar Ruse

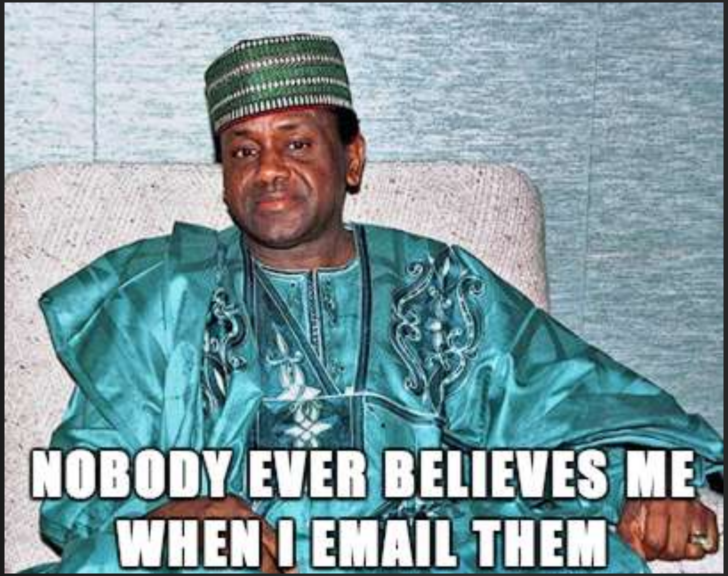
- Needs to look legit
- Needs to trigger a response
- Needs to create urgency
- Needs to go undetected
- Needs to avoid red flags

Don’t email, inject event!



Calendar Event Injection

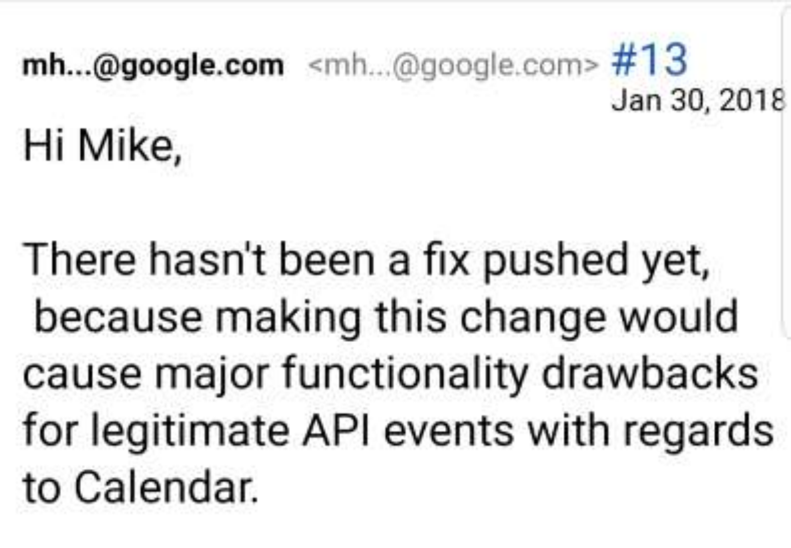
- Silently inject events into calendars
- Creates urgency via reminders
- Include link to phishing page
- Mass-exploitation w/o visibility
- Litter calendars for the future
- Remove traces by erasing the event
- Include GoToMeeting
  - Don't forget to record the meeting! :)
- How did we get here???



Calendar Event Injection

- Fun w/ the Google API
- Mark victims as ‘Accepted’
- Add comments for victims
- but.. they never receive an invite
- Bypasses setting for not auto-add
- Reported 10/9/2017

Google Isn’t Patching!

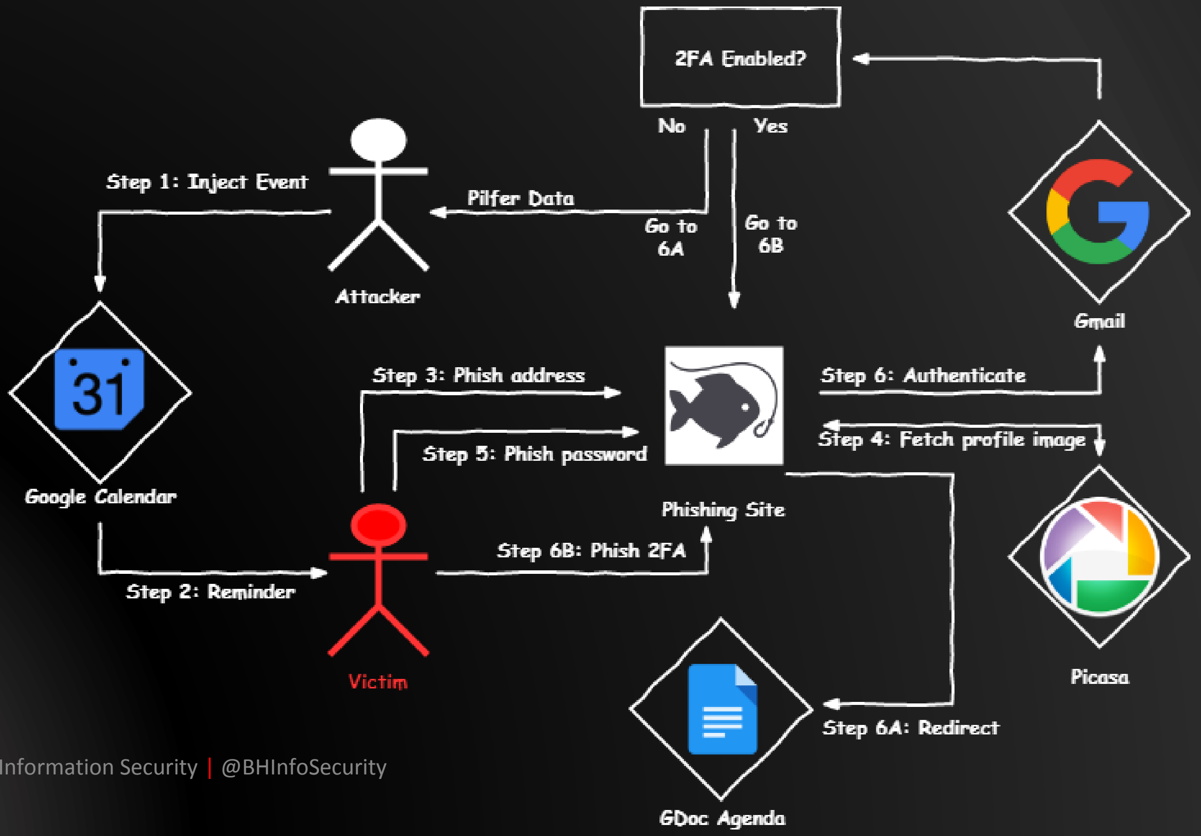


mh...@google.com <mh...@google.com> #13
Jan 30, 2018

Hi Mike,

There hasn't been a fix pushed yet, because making this change would cause major functionality drawbacks for legitimate API events with regards to Calendar.

Personalized Phishing

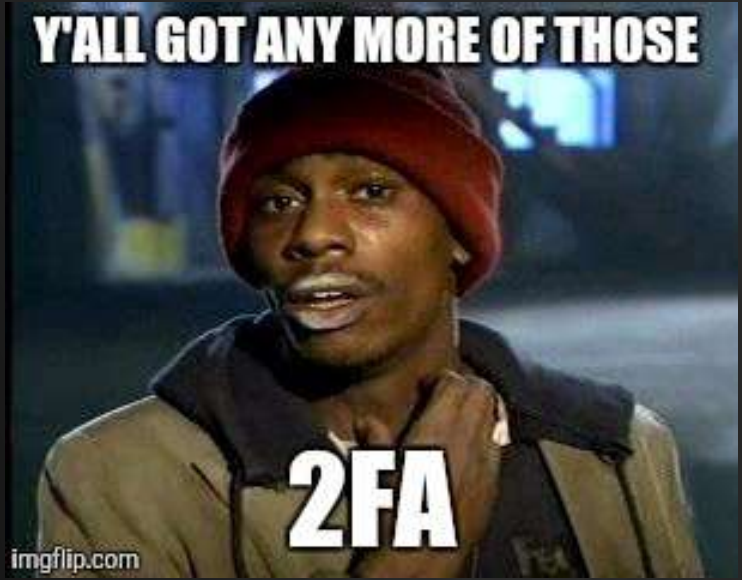


Google 2FA Requirements

Username + Password + ...

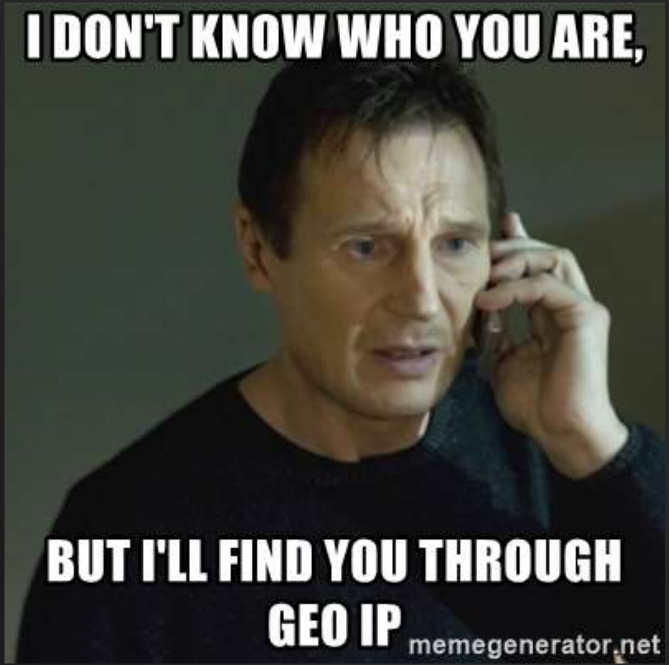
- SMS: Text Message
- TOTP: Google Authenticator
- Phone Prompt: Touch Phone
- U2F: Hardware Device

Challenge Accepted!



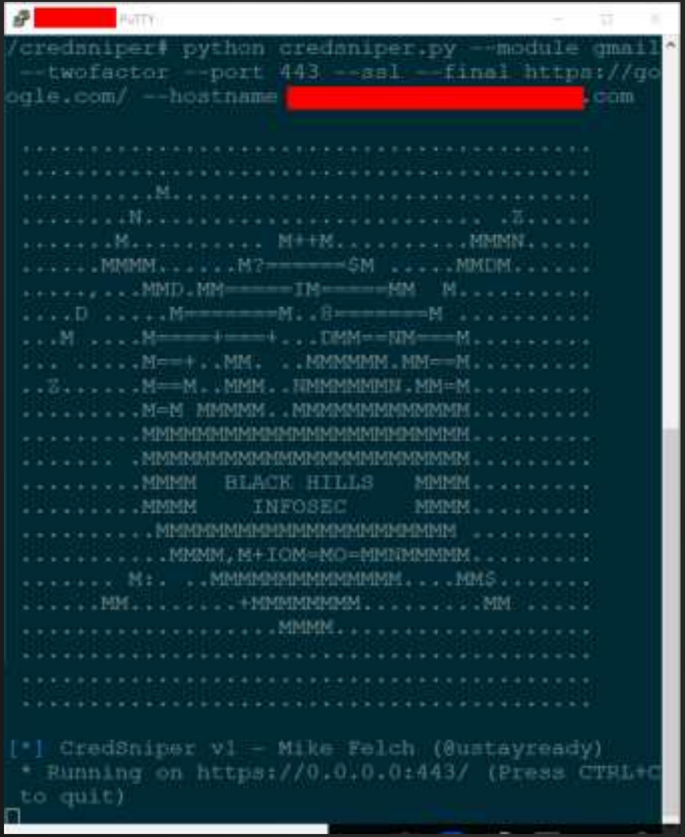
Additional 2FA Points

- Might get asked for last location
  - GeoIP it from IP during capture
- Immediately clear red alert bar
  - Clear for one, clear for all
- Multiple failed phone prompts
  - Disables phone prompt for few hours
  - Automatically switches 2FA option
  - May also contain attacker location/device



Quick CredSniper Intro

- Fetch the profile image
  - Google Picasa API
  - JavaScript XMLHttpRequest()
- Ask nicely for the password
- Behind the scenes, authenticate
  - Is 2FA present?
  - No? Redirect them to GDoc agenda
- Doh! 2FA is enabled
  - Which type? Extract information
- Ask for 2FA Token nicely
  - Login w/ Username + Password + Token



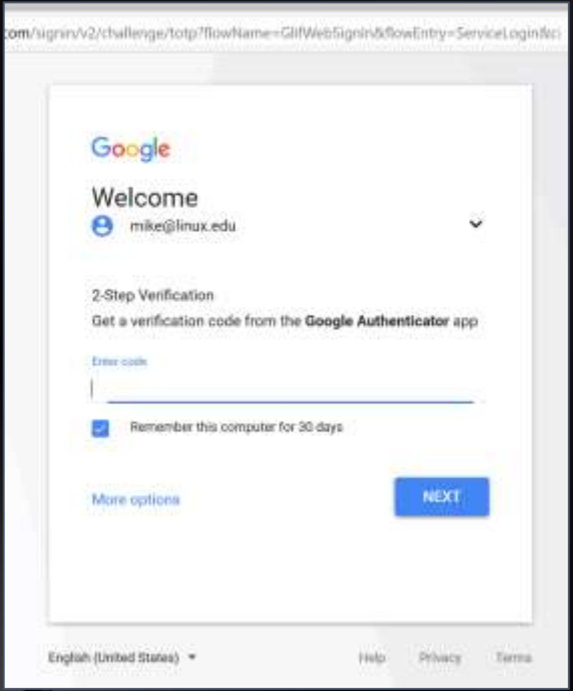
```
/credsniper# python credsniper.py --module gmail
 --twofactor --port 443 --ssl --final https://go
ogle.com/ --hostname [redacted].com

 ..........................................
 ..........................................
 ..........M...............................
 .........N.......................... .Z......
 ........M........... M++M.........MMMMN.....
 .......MMMM.......M?========$M ......MMDM......
 .......,...MMD.MM======IM======MM  M..........
 ....D .....M========M..8========M ..........
 ...M ....M=====+=====+...DMM==NM====M.........
 ... ......M==+..MM.  ..MMMMMM.MM==M.........
 ..Z.......M==M..MMM..NMMMMMMMN.MM=M.........
 ..........M=M MMMMM..MMMMMMMMMMMMMM.........
 ..........MMMMMMMMMMMMMMMMMMMMMMMMM.........
 ........ .MMMMMMMMMMMMMMMMMMMMMMMMM.........
 ..........MMMM  BLACK HILLS   MMMM.........
 ..........MMMM    INFOSEC     MMMM.........
 ...........MMMMMMMMMMMMMMMMMMMMMMM .........
 ............MMMM,M+IOM=MO=MMNMMMMM.........
 ....... M:.  ..MMMMMMMMMMMMMMM....MMS........
 ......MM.........+MMMMMMMM.........MM .....
 .....................MMMM.....................
 ..........................................

 ..........................................
 ..........................................

[*] CredSniper v1 - Mike Felch (@ustayready)
 * Running on https://0.0.0.0:443/ (Press CTRL+C
 to quit)
```

CredSniper for teh win



om/signin/v2/challenge/totp?flowName=GlifWebSignIn&flowEntry=ServiceLogin&c

Google

Welcome

mike@linux.edu

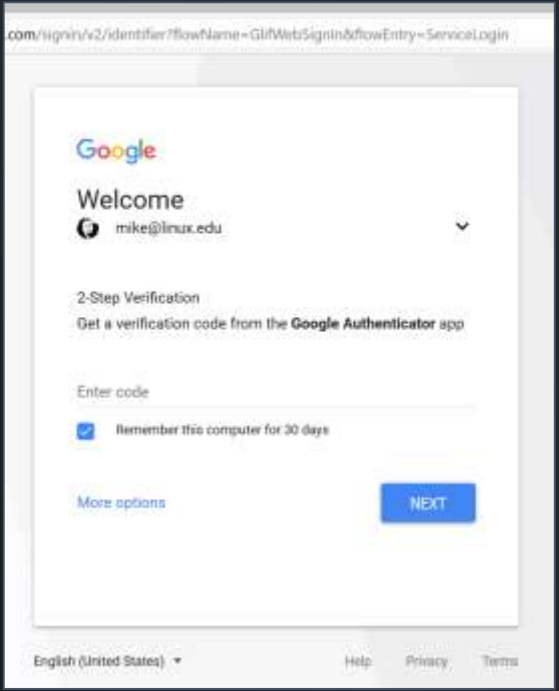
2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code

☑ Remember this computer for 30 days

Real Or Fake?



.com/signin/v2/identifier?flowName=GlifWebSignIn&flowEntry=ServiceLogin

Google

Welcome

mike@linux.edu

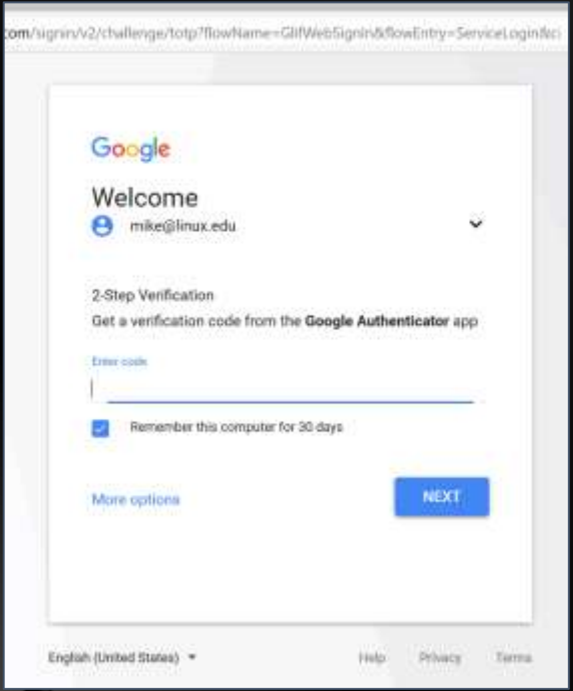
2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code

☑ Remember this computer for 30 days

CredSniper for teh win



com/signin/v2/challenge/totp?flowName=GlifWebSignIn&flowEntry=ServiceLogin&c

Welcome

mike@linux.edu

2-Step Verification

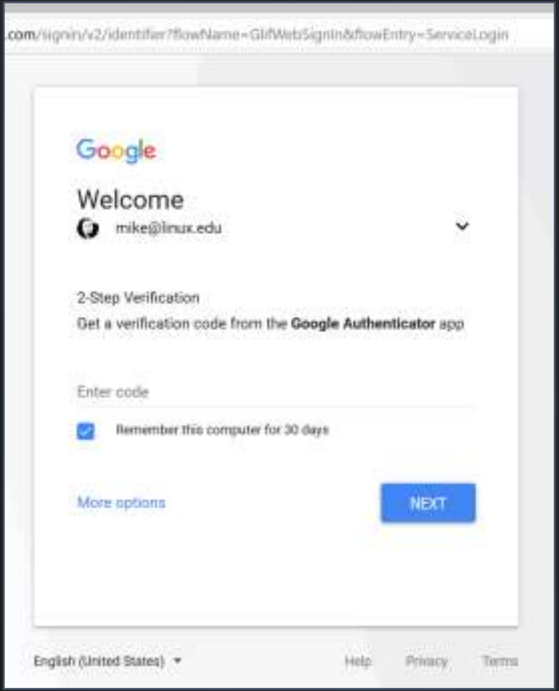
Get a verification code from the **Google Authenticator** app

Enter code

☑ Remember this computer for 30 days

Real

Real Or Fake?



.com/signin/v2/identifier?flowName=GlifWebSignIn&flowEntry=ServiceLogin

Welcome

mike@linux.edu

2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code

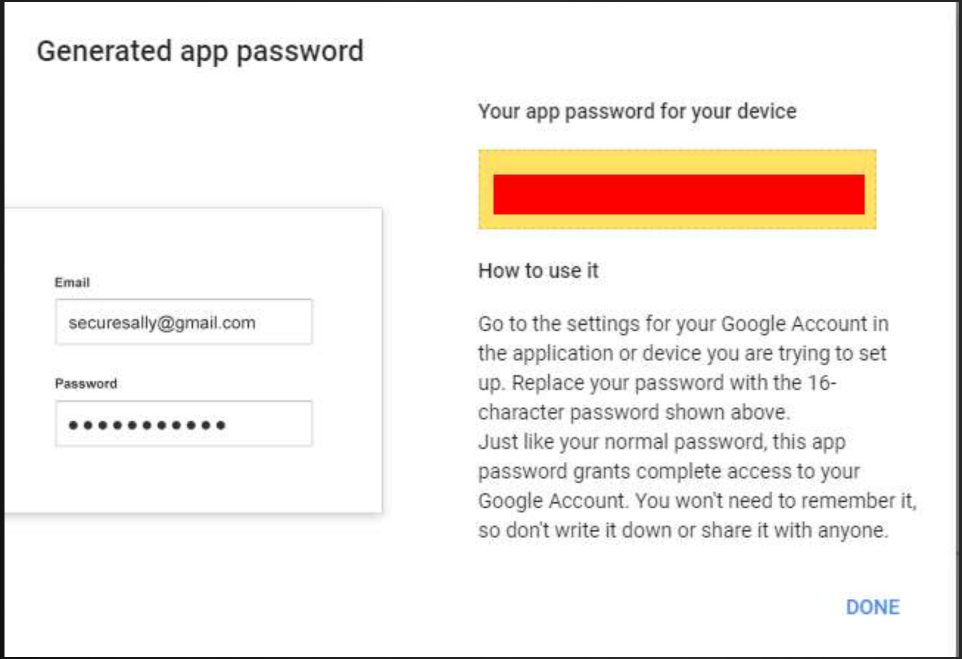
☑ Remember this computer for 30 days

Fake

Persistence:
Hide in Plain Sight

Generate App Password

- Backdoor password for account
- Under ‘My Account’
  - Click ‘Sign-in & Security’
    - Select ‘App-Passwords’
- Combine w/ 2FA backdoor
- Login as normal after triage!



Generated app password

Email

securesally@gmail.com

Password

●●●●●●●●●●●●

Your app password for your device

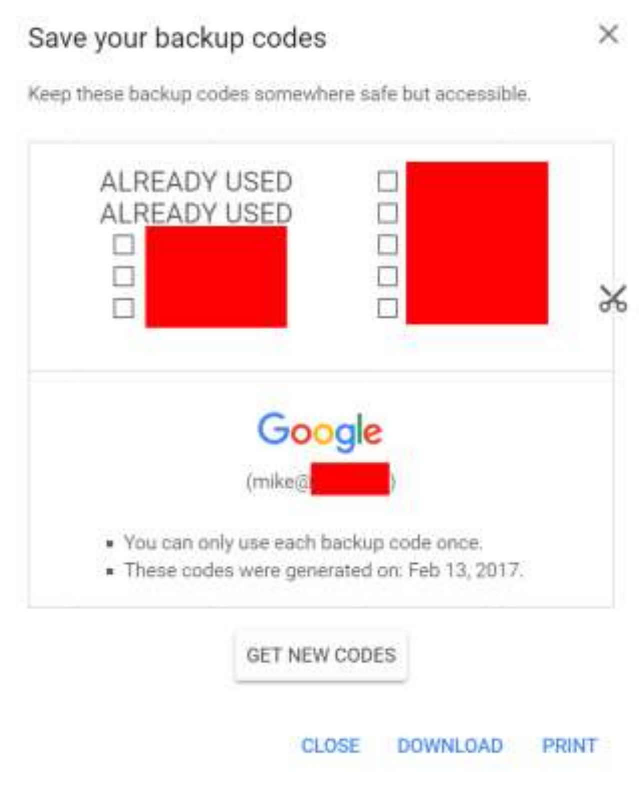
[redacted]

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.
Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

Backup Codes

- Download alternative 2FA tokens
- Rarely get re-generated after breach
- Most don't know they even exist
- Great combined w/ app passwords!



Save your backup codes

Keep these backup codes somewhere safe but accessible.

ALREADY USED
ALREADY USED
□
□
□ [redacted]

□
□
□
□
□ [redacted]

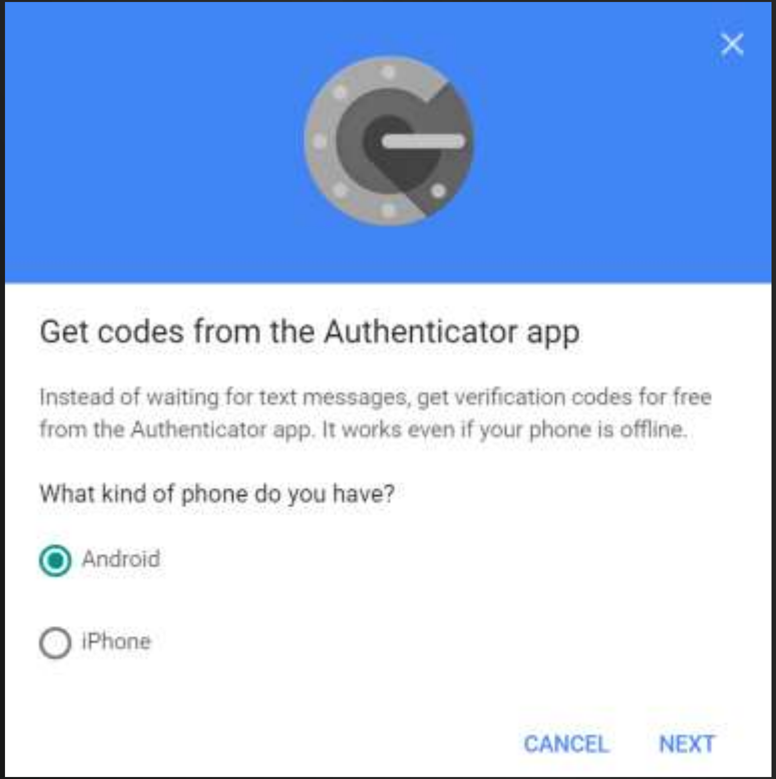
Google

(mike@[redacted])

- You can only use each backup code once.
- These codes were generated on: Feb 13, 2017.

Enroll New 2FA Device

- Tie 2FA to your own device
- Generate legit 2FA tokens
- Commonly gets inspected after breach
- Nice when undetected though...



Get codes from the Authenticator app

Instead of waiting for text messages, get verification codes for free from the Authenticator app. It works even if your phone is offline.

What kind of phone do you have?

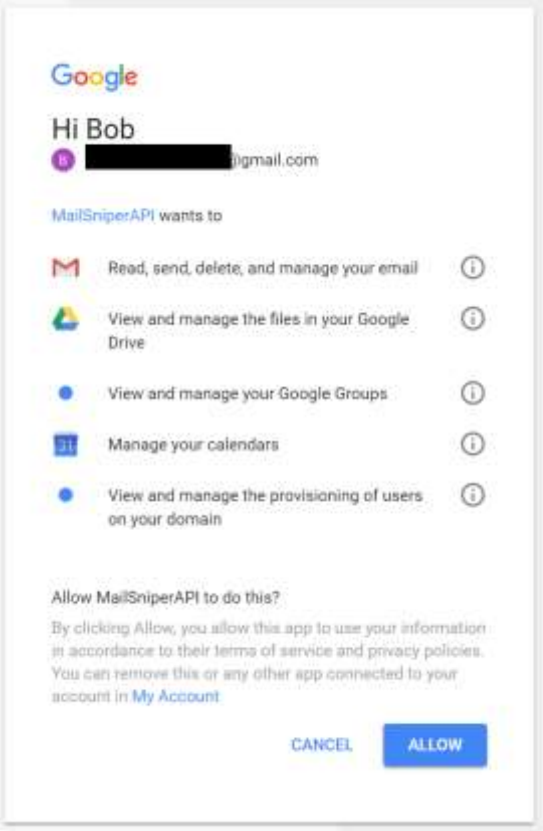
● Android

○ iPhone

Authorized API Backdoor

- Sign-up a new project on cloud.google.com
- Enable API access
- When creating API client, add full scopes
- Sign-in to victim account and authorize backdoor app!

```
SCOPES =  '
   https://www.googleapis.com/auth/calendar
   https://mail.google.com/
   https://www.googleapis.com/auth/drive
   https://www.googleapis.com/auth/groups
   https://www.googleapis.com/auth/admin.directory.user
'
```



Google

Hi Bob

[redacted]@gmail.com

MailSniperAPI wants to

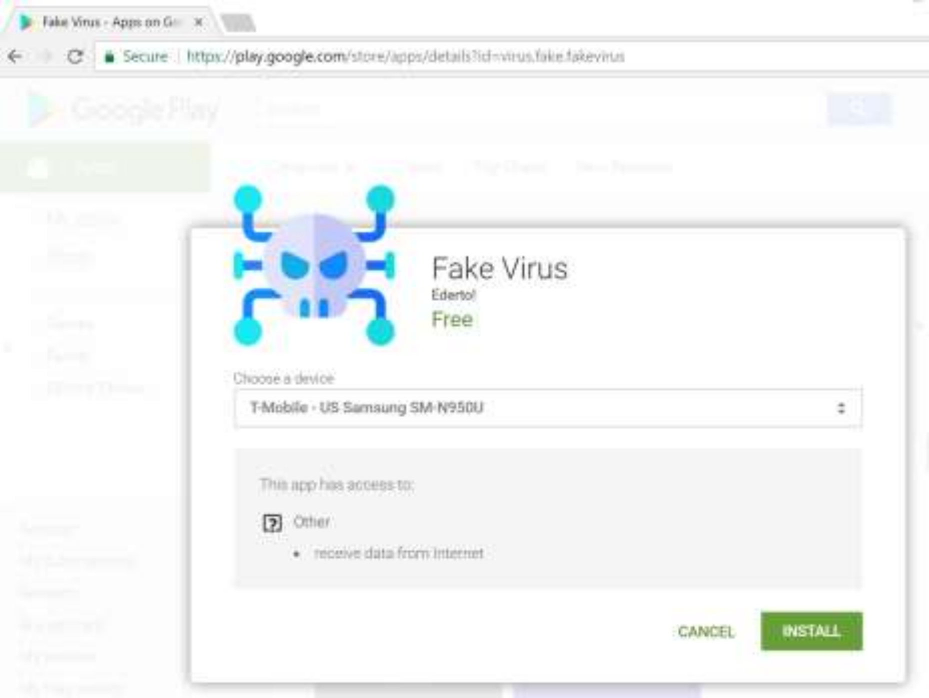
- Read, send, delete, and manage your email
- View and manage the files in your Google Drive
- View and manage your Google Groups
- Manage your calendars
- View and manage the provisioning of users on your domain

Allow MailSniperAPI to do this?

By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in My Account

Backdoor Android App

- Don't Publish app in Play Store
- Login to victim account
- Browse to app in Play Store
- Install to victims mobile device
- Pop a shell!
- Pilfer, persist and pivot..



Fake Virus - Apps on G

Secure | https://play.google.com/store/apps/details?id=virus.fake.fakevirus

Google Play

Fake Virus

Edertol

Free

Choose a device

T-Mobile - US Samsung SM-N950U

This app has access to:

Other

- receive data from Internet

Demo:
Malicious Android App

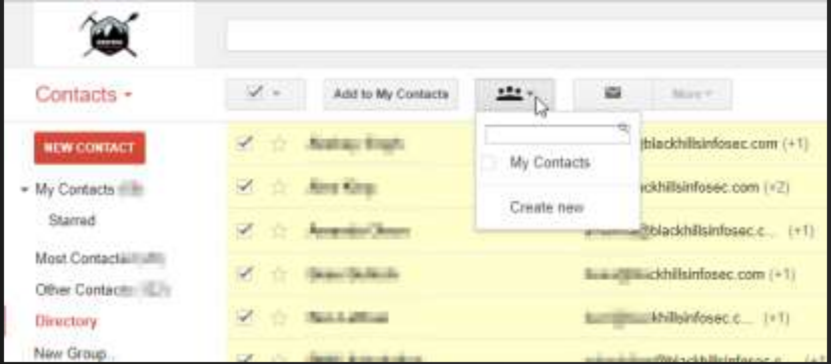
Re-configure Account

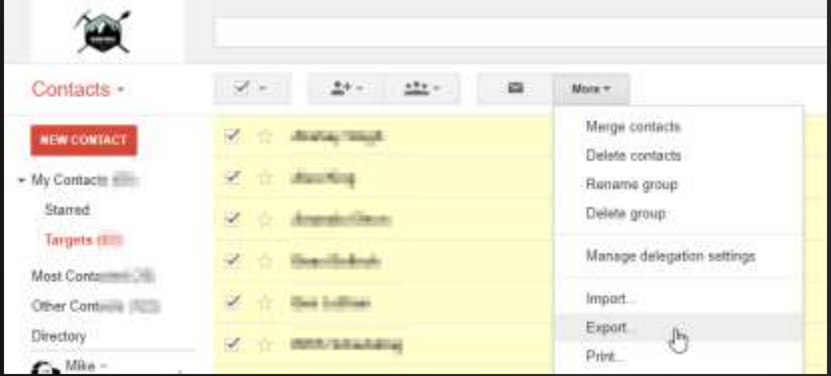
- Add email rules to delete alerts
  - no-reply@accounts.google.com
- Add recovery email/phone
- Create email forwarder
  - Monitor for global SOC emails :)
- Add calendar events for others
- Delegate account to another victim
- Locked out? Recover account!

Internal: Collateral Damage

Target Company Directory

- Create contacts group from directory
- Export all the contacts
- Tailor your target list..
- More technical, more access!
- Create a LinkedIn doppelganger
  - Side note.. file transfers don't have [EXTERNAL] tags like email



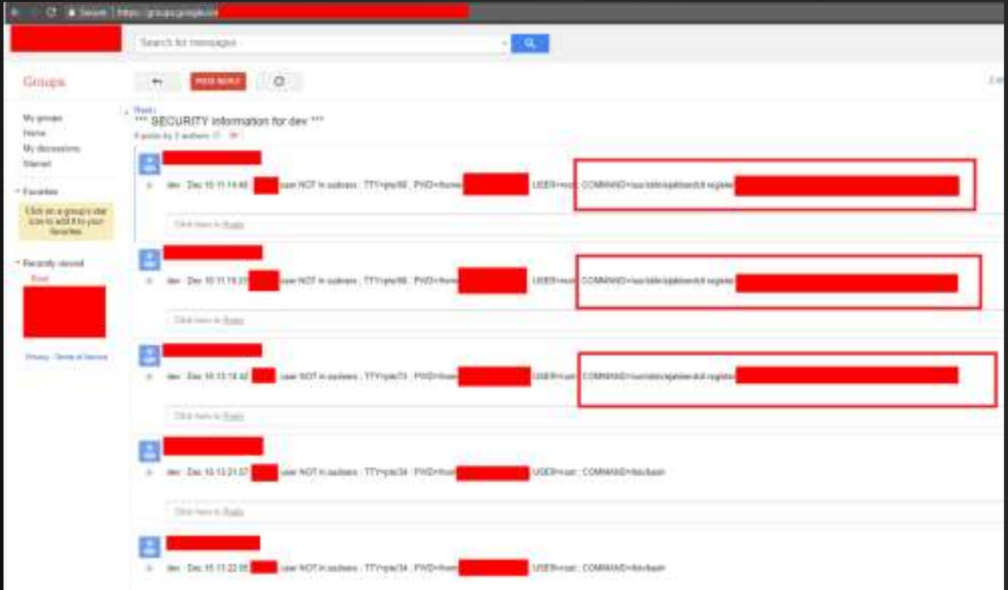


Search Gdrive/Gmail

- Search for files with ‘password’
  - Download a zip of them all!
- Any VPN documentation?
- What 3rd party sites do they use?
- Files with ‘confidential’ in the title
- Credit card keywords...
- AWS access_key/secret_access_key
- MailSniper supported!

Find Google Groups

- Go to groups.google.com
- Groups might not be listed
- You can still can search!
- Look for keywords:
  - access_key
  - password
  - root
  - ...etc
- Devs LOVE groups for cron


Secure | https://groups.google.c[redacted]
[redacted]
Search for messages
Groups
POST REPLY
My groups
Home
My discussions
Starred
Favorites
Click on a group's star icon to add it to your favorites
Recently viewed
[redacted]
Privacy - Terms of Service

*** SECURITY information for dev ***

[redacted]

```
dev : Dec 15 11:14:40 [redacted] user NOT in sudoers ; TTY=pts/0 ; PWD=/home/[redacted] USER=root ; COMMAND=/usr/sbin/[illegible] register [redacted]
```

Click here to Reply

[redacted]

```
dev : Dec 15 11:19:2[illegible] [redacted] user NOT in sudoers ; TTY=pts/0 ; PWD=/home/[redacted] USER=root ; COMMAND=/usr/sbin/[illegible] register [redacted]
```

Click here to Reply

[redacted]

```
dev : Dec 15 13:14:42 [redacted] user NOT in sudoers ; TTY=pts/3 ; PWD=/home/[redacted] USER=root ; COMMAND=/usr/sbin/[illegible] register [redacted]
```

Click here to Reply

[redacted]

```
dev : Dec 15 13:21:07 [redacted] user NOT in sudoers ; TTY=pts/4 ; PWD=/home/[redacted] USER=root ; COMMAND=/bin/bash
```

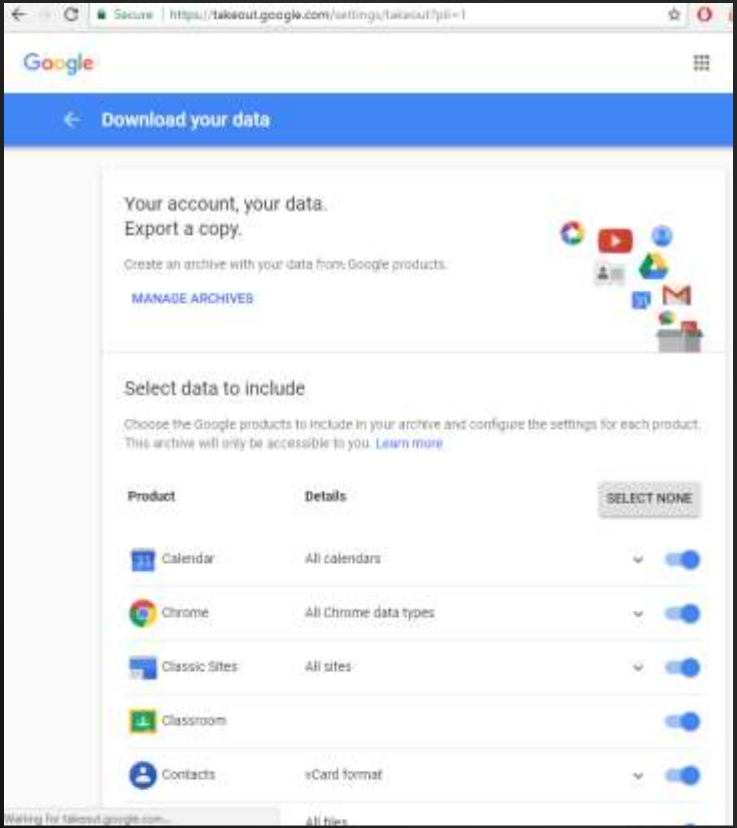
Click here to Reply

[redacted]

```
dev : Dec 15 13:22:05 [redacted] user NOT in sudoers ; TTY=pts/4 ; PWD=/home/[redacted] USER=root ; COMMAND=/bin/bash
```

Eat the whole elephant

- https://takeout.google.com
- Export all Google data from an account
- Includes:
  - All G-Drive files, full search history, Hangouts message data, all emails, all calendar events, Voice history, etc…



Download your data

Your account, your data.
Export a copy.

Create an archive with your data from Google products.

MANAGE ARCHIVES

Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. Learn more

SELECT NONE

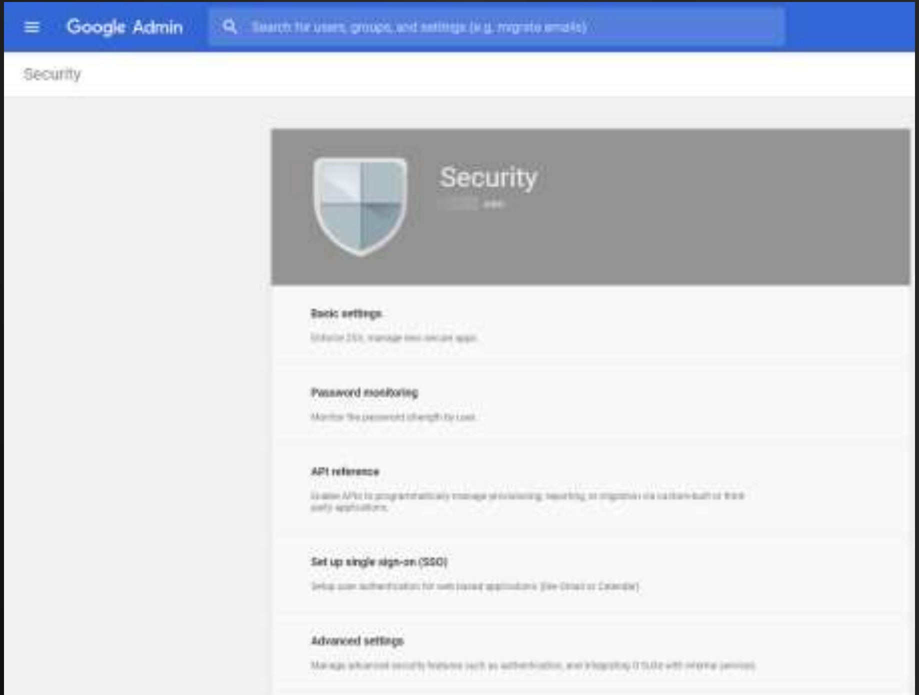
Product	Details
Calendar	All calendars
Chrome	All Chrome data types
Classic Sites	All sites
Classroom	
Contacts	vCard format
	All files

Waiting for takeout.google.com...

Pop Google Admin

- Manage All Users
- Manage All Domains
- Manage All Files
- Manage All SSO/Auth
- Manage All Devices

Game Over!



Google Admin
Search for users, groups, and settings (e.g. migrate emails)
Security
Security

Basic settings
Enforce 2SV, manage less secure apps.

Password monitoring
Monitor the password strength by user.

API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third party applications.

Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar)

Advanced settings
Manage advanced security features such as authentication, and integrating G Suite with internal services.

Defending:
Triage the Breach

Reset Accounts

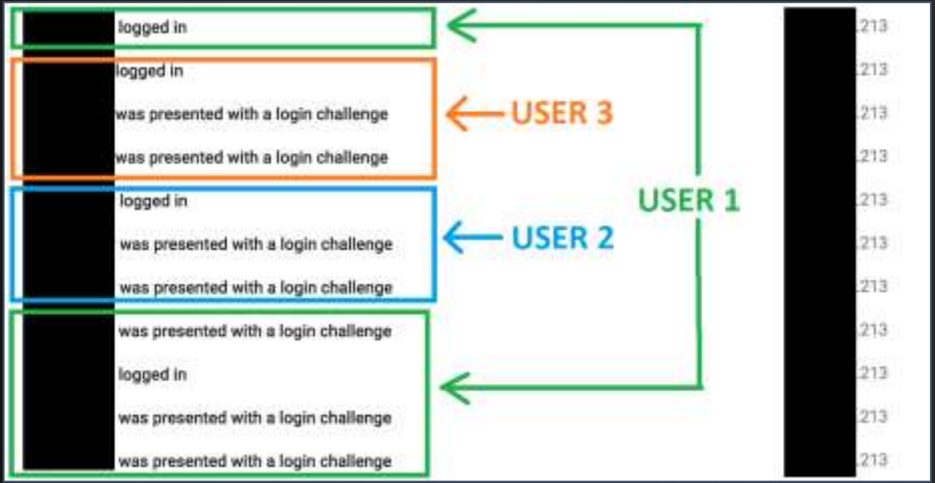
- Log out of all sessions
- Change user password
- Generate new backup codes
- Capture IoC for threat hunting
- … anything else?

Look for Backdoors

- Remove app passwords
- Remove 2FA devices
- Remove authorized apps
- Remove email forwarders
- Remove email filters
- Remove bad recovery email/phone
- Remove bad Android apps
- Remove bad account delegations

Find Victims & Monitor

- Get familiar with Google Admin console
  - https://github.com/jay0lee/GAM
- Search by IP address
- Don't just change passwords
  - Remove backdoors
  - Look for rogue email forwards
  - Generate a timeline
- Communicate better!



[redacted]

```
logged in                                  213
logged in                                  213
was presented with a login challenge       213
was presented with a login challenge       213
logged in                                  213
was presented with a login challenge       213
was presented with a login challenge       213
was presented with a login challenge       213
logged in                                  213
was presented with a login challenge       213
was presented with a login challenge       213
```

[redacted]

Finishing Up:
Questions for You

Question to GSuite Users

Does your BYOD policy give you the ability to test/audit security for corporate email and files on personal devices? What about corporate phones? Should it?

Are employees just trained on phishing/SE ‘red flags’ or are they taught good user-behavior patterns?

How strong is your password policy or are you just trusting in Google?

Question to Google

- GSuite customers need a process that allows us to submit approval requests for pentests engagements. Testing our configurations, users, devices and data is important to us. Help us keep our engagements transparent to you, above board, and without getting suspended for alleged TOS violations.

Can you implement an engagement approval process?

Questions?

- Twitter
  - Mike - @ustayready
  - Beau - @dafthack
  - BHIS - @BHInfoSecurity
- Black Hills Information Security
  - http://www.blackhillsinfosec.com/
- MailSniper
  - https://github.com/dafthack/MailSniper
- CredSniper
  - https://github.com/ustayready/CredSniper
- CredKing
  - https://github.com/ustayready/CredKing