The Clouds.. The Clouds Are Out To Get Me.

Or, all my best presentations are done at 4AM the day I am presenting...
TWO POLISCI MAJORS IN A ROW AT A HACKER CONFERENCE?

THAT IS INTERESTING!
So... Why This Topic?

- Because, we are getting into some really bad loops in pentesting
- Phish > Internal Access > Pivot > Elevate > Repeat
- I have a fear we are getting stale
- I have a fear cloud-based issues are more difficult to understand
- Josh Wright’s Law
- There is so much more out there.....

“That’s a cute attack, is there a Metasploit module for it?”
Way back in 2008...... A wise man said...

The Primacy of Passwords

- Passwords remain the dominant form of user authentication today
  - On intranets, certainly
  - But, often on internet-accessible systems, as well:
    - VPNs, SSH, web applications, email access, and such
- Professional network penetration testers and ethical hackers must understand password attacks at a fine-grained level
  - They make up a crucial component of our arsenal
- "When I started pen-testing, I was under the impression that exploits were the stuff. In fact, it wasn't until my first pen-test with [infosec luminary] that he was able to put me at ease by saying it outright ... passwords are a huge part of penetration testing." --Professional Penetration Tester
Let’s Dive in With Creds, Creds are King

- BHIS has tremendous luck password spraying
- Thanks Microsoft and Google!!!
- Why? Why does an attack that was in the original OWASP Top 10 still work today?
- “It’s OK if you have 2FA!”*
- Use Hydra and/or Burp
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.
“Not a problem.” - Google

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 - 5am</td>
<td>Google Says</td>
</tr>
<tr>
<td>5 - 6am</td>
<td>That</td>
</tr>
<tr>
<td>6 - 6:45am</td>
<td>This</td>
</tr>
<tr>
<td>7 - 8am</td>
<td>Not</td>
</tr>
<tr>
<td>8:30 - 9:15am</td>
<td>Anyone</td>
</tr>
<tr>
<td>9:30 - 10:15am</td>
<td>Ever</td>
</tr>
<tr>
<td>10:30am</td>
<td>Worried, 10:30am</td>
</tr>
<tr>
<td>11am</td>
<td>About</td>
</tr>
<tr>
<td>11:30am</td>
<td>Ever, 11:30am</td>
</tr>
<tr>
<td>December 5th 2020</td>
<td>Is, 12pm</td>
</tr>
<tr>
<td></td>
<td>Going to freak, 12:30pm</td>
</tr>
<tr>
<td></td>
<td>Me out, 1pm</td>
</tr>
<tr>
<td>6:30 - 7:30am</td>
<td>Is</td>
</tr>
<tr>
<td>7:30 - 9am</td>
<td>A Problem</td>
</tr>
<tr>
<td>9 - 9:45am</td>
<td>Should</td>
</tr>
<tr>
<td>10 - 10:45am</td>
<td>Be</td>
</tr>
</tbody>
</table>
Enter, Credsniper

Pretty Much Self Explanatory

Attacking Google 2FA

@daftback and @ustaready. In their natural environment.

Pretty Much Self Explanatory
Credsniper Simplified

- Sets up a phishing server
- Captures 2FA
- Bypasses U2FA
- Suppresses all Google security alerts
- Creates a App password
- Pillage?
- Everything connected to Google auth… Is everything.
Get Credsniper Now...

- 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
- [https://www.slideshare.net/dafthack/ok-google-how-do-i-red-team-gsuite](https://www.slideshare.net/dafthack/ok-google-how-do-i-red-team-gsuite)

https://github.com/ustayready/CredSniper
A Very Special Heads Up

- Please be careful
- Google does not “like” this
- Something about violating terms of service
- This gets into much larger issues later
- They will ban you, your family and any of your pets that have Google accounts at your location

Angering Fortune 100 companies can have consequences
What We Learned From Watching Bad Movies..
Enter CredKing

- Determine naming convention
- Search LinkedIn for users
- Generate email lists
- Try one password at a time
- Spray all the accounts regularly
- https://github.com/ustayready/CredKing
The Point????

“I need a iPhone 0-day ASAP!!”

Vrs..

“His password was Furries4Ev3r”
What then? - Mailsniper

- For the tester who wants to bypass OWA 2FA
- For the tester that wants to search email for individual users, or an entire organization
- For the tester who wants to find all inboxes which have delegated their inbox to... Everyone
- For the tester who wants to password spray a GAL
- https://github.com/dafthack/MailSniper

For all the testers... All the time
Azure

- Azure.. What the hell?
- From the Internet you can pull:
  - Users
  - Groups
  - Group Membership
  - Service Principals
  - Applications
- And… Add guest users
- All with a standard user account
- One week of research


I am sure this is all vetted and secure….
The Browser is the New Endpoint

- **Outlook add-ins**
  - Get creds > Login to O365 > Add add-in > Add-in syncs everywhere
  - Oh.. The Outlook Desktop client uses Edge… So it works there
  - Add-in to BeEF Hook
  - Add-in to harvest creds
  - ???
  - [https://www.slideshare.net/dafthack/covert-attack-mystery-box-a-few-novel-techniques-for-exploiting-microsoft-features](https://www.slideshare.net/dafthack/covert-attack-mystery-box-a-few-novel-techniques-for-exploiting-microsoft-features)

- **Ever think about Grammarly?**
  - It is a keylogger

- **What about LastPass?**
  - It monitors every page you go to
Why This Matters

- Many of these attacks are not “straight forward”
- They require a bit of setup
- They are devastatingly effective
- They are also just the tip of the iceberg
- We need to move out of what is comfortable
- The cloud is crazy
- Embrace it

“Back again”
A Special Note on Non-Attribution

- I went off the blockchain deep end
- I wanted to go full non-attrib
- It… Did not go well
  - Unless you want to pay a 60% “transaction” fee
  - Which I did not
- But, the Internet is a wonderful place
- It is also insane and has ICP clowns

Want to buy some Bitcoin?
Not Proud of This at All…. Step One..
Problem.. No
But…

Totally Cool…
Site Seems Legit..
Would You Like to Buy Some Bitcoin?

“But I don’t want to go among mad people,” Alice remarked. “Oh, you can't help that,” said the Cat: “we're all mad here.”
Thanks!

- Let’s take apart the cloud....
- Science is failing and taking notes.
- John Strand
- @strandjs
- john@blackhillsinfosec.com