How we hacked your billion-dollar company for forty-two bucks

or, getting a foothold inside the perimeter

jamie.riden@ioactive.com

IOActive®

Outline

about me

background

four cases where the client thought the perimeter was fine

… and why it was not fine

absolutely no Cobalt Strike

questions

curriculum vitae – ’95 to present

maths / CS degree

adequate C++/Java developer

sysadmin / blue team

penetration tester since 2010

passed CCSAS 2014 & CSAM 2015, didn’t actually do RT til 2018, so relative newcomer

composition of a red team
(brief digression / rant)

it can seem a bit like “all you need to start doing RT is 2 years experience doing RT”

obviously, you need to balance training newer people with delivering a good service

but equally, new people bring in new ideas

Preamble

“... there are people who will try anything to secure their networks, except design them correctly, control the access levels within them, segment their networks, understand their traffic, and monitor things closely." – Marcus J Ranum, Silver Bullet Podcast

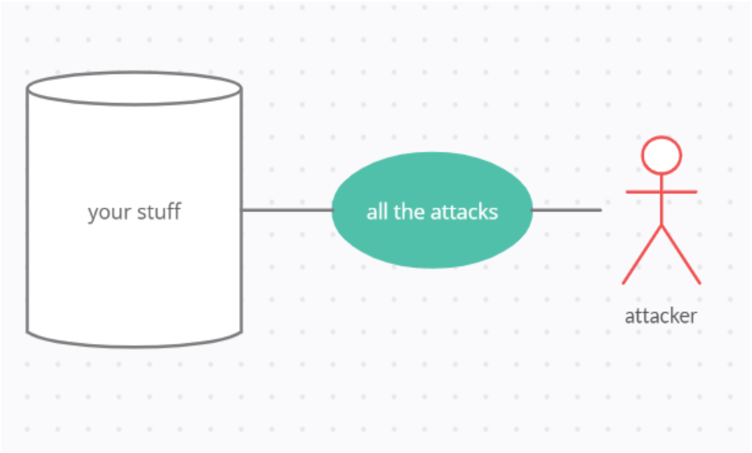
but of course, everyone is under pressure to deliver new things and little time is left to check things are as they should be.

Objective / Threat Model

Try all the possible ways to compromise the client

Stop when one works

subvert (v) : to undermine the principles of; corrupt.



Can you be a bit more specific?

The perimeter is permeable:

- email goes in and out
- web traffic goes out and in (from corp to Internet)
- web traffic goes in and out (from Internet to “DMZ”)
- VPNs, helpdesk services – specially password reset, cloud auth, Citrix, file exchange, dev boxes, etc.

Can we chain issues to get in ? spoiler: yes, in 4/5 cases

How to compromise the target

Physical?
I’m too lazy / COVID

0-days? Too hard

Dropped USB sticks?
Risky and ineffective

In-house web apps

Misconfigured/forgotten assets

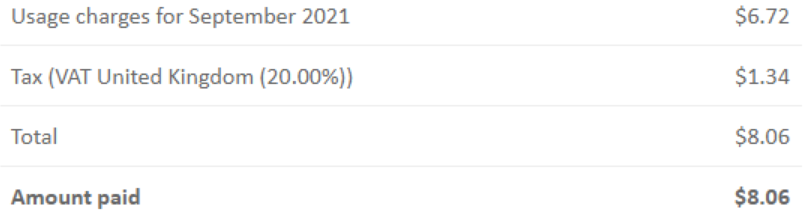
Unforeseen interactions

Issues are rarely independent of each other

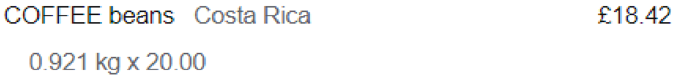
(a good hold which you can’t reach, isn’t any use; a bad hold can be enough to move up)

What we needed

- VPS or other Linux box on the Internet (~8$/month)
- Domain name (~10 USD a pop)
- AWS account for Fireprox (couple of bucks / month)
- scripting language
- Google
- patience
- caffeine not included



Usage charges for September 2021	$6.72
Tax (VAT United Kingdom (20.00%))	$1.34
Total	$8.06
Amount paid	**$8.06**



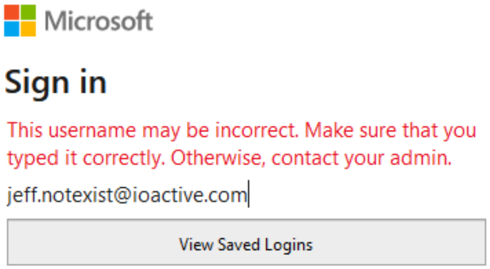
COFFEE beans	Costa Rica	£18.42
0.921 kg x 20.00		

Defining some terms: User Enumeration

Term used where some function confirms a username is valid or not:

- password reset : doesn't exist vs. we sent you email
- timing attacks : valid user details need to be looked up
- for example office.com / MSOL login

We just need some observable difference.



Sign in

This username may be incorrect. Make sure that you typed it correctly. Otherwise, contact your admin.

jeff.notexist@ioactive.com

Password spraying

First, find a lot of valid user IDs

Try e.g. “Winter2021!” against each in turn

When finished, think of a new password guess

Evades naïve AD lockout counter (N tries / user / time)

May need Fireprox to evade rate limiting e.g. on MSOL

MonthYear, SeasonYear!, Welcome123, Trump2020, etc.

First example - TAHI.com

On premise Exchange, circa 10k users.

OSINT / FOCA got examples that looked like user IDs

Helpdesk web page allowed enumeration of users

e.g. ID01234567 – bash script to create ID0123????

Password spraying via SprayingToolkit / MailSniper

TAHI – Username Enum via OWA

```
PS MailSniper> Invoke-UsernameHarvestOWA -
ExchHostname mail.tahi.com -Domain TAHI -UserList
tahi-users.txt -Threads 3 -outfile actualusers.txt

[*] Now spraying the OWA portal at
https://mail.tahi.com/owa/

Determining baseline response time...

Response Time (MS)          Domain\Username

3700                        TAHI\efgHbJ

[*] Potentially Valid! User:TAHI\u13301

983                         TAHI\u13301
```

TAHI – OWA and EWS Spraying

```
PS MailSniper> Invoke-PasswordSprayOWA -
ExchHostname mail.tahi.com -UserList .\userlist.txt
-Password Spring2021! -Threads 5 -OutFile sprayed-
owa-creds.txt
```

[EWS is EXCHANGE WEB SERVICES]

```
PS MailSniper> Invoke-PasswordSprayEWS -
ExchHostname mail.domain.com -UserList
.\userlist.txt -Password Spring2021 -Threads 15 -
OutFile sprayed-ews-creds.txt
```

Patience needed, but not that difficult

Started using MailSniper to enumerate on 16th of the month;

Got nearly 1,000 valid users.

List used for password spraying – evading standard AD lockout

On 22nd of the month, two passwords were obtained.

OWA did not have 2 Factor Auth; we’re in.

Internal mail filtering a lot less restrictive than from outside

Drop a custom implant in a reply, ask victim to open.

Second example - RUA.com

Used FOCA to establish a few examples (“jsmith”)

MSOLSpray.py w/ fireprox used to trawl through generated candidates

(https://americansurnames.us/top-surnames)

Oh no! – login involves redirect to on-prem IDP / ADFS

MSOLSpray.py gives existence, but **does not confirm correct password**

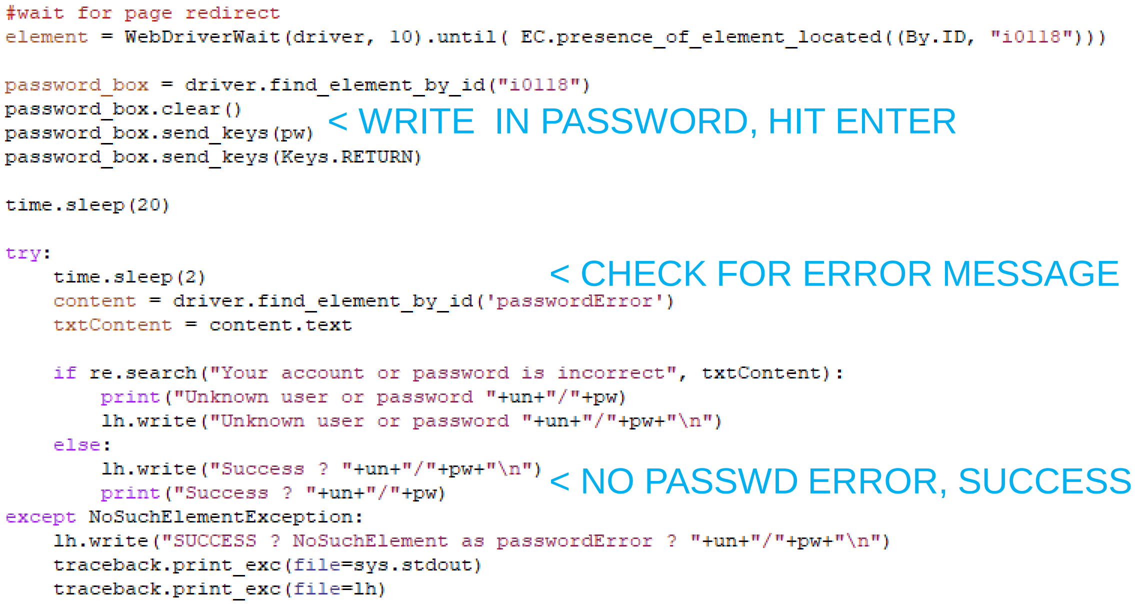
Needed to think how to fix that.

Tools – MSOLSpray.py

```
$ python3 MSOLSpray.py -v --userlist userguesses.txt --
password "November2021!" --sleep 10 --url
https://c5go9url1a.execute-api.us-east-
1.amazonaws.com/fireprox

Now spraying Microsoft Online.

Current date and time: Mon Oct 26 06:13:49 2020

WARNING! The user asmith@rua.com doesn't exist.

VERBOSE: Invalid username or password.

Username: jsmith@rua.com could exist.

..
```

Selenium & Python to the rescue

We drive the browser through the whole process, step by step.



```
#wait for page redirect
element = WebDriverWait(driver, 10).until( EC.presence_of_element_located((By.ID, "i0118")))

password_box = driver.find_element_by_id("i0118")
password_box.clear()
password_box.send_keys(pw)
password_box.send_keys(Keys.RETURN)

time.sleep(20)

try:
    time.sleep(2)
    content = driver.find_element_by_id('passwordError')
    txtContent = content.text

    if re.search("Your account or password is incorrect", txtContent):
        print("Unknown user or password "+un+"/"+pw)
        lh.write("Unknown user or password "+un+"/"+pw+"\n")
    else:
        lh.write("Success ? "+un+"/"+pw+"\n")
        print("Success ? "+un+"/"+pw)
except NoSuchElementException:
    lh.write("SUCCESS ? NoSuchElement as passwordError ? "+un+"/"+pw+"\n")
    traceback.print_exc(file=sys.stdout)
    traceback.print_exc(file=lh)
```

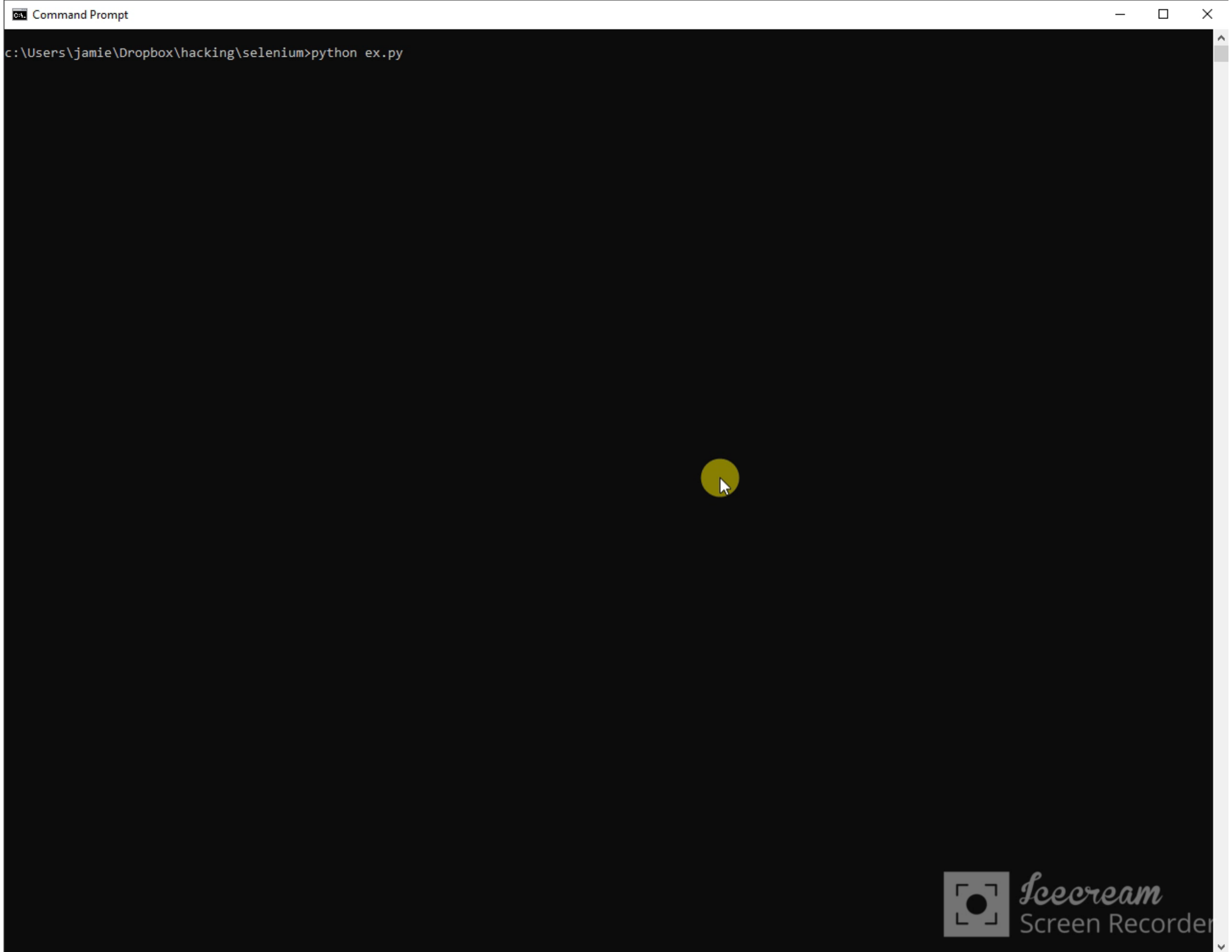
< WRITE IN PASSWORD, HIT ENTER

< CHECK FOR ERROR MESSAGE

< NO PASSWD ERROR, SUCCESS ?

IOActive.

DEMO



```
c:\Users\jamie\Dropbox\hacking\selenium>python ex.py
```

Back to RUA

Using OSINT we got some example UIDs and generalised

Using MSOLSpray we got a couple of thousands of usernames

Using selenium we got correct passwords for maybe 10

2FA had been enabled, with registration on FIRST LOGIN

Nature of business meant a lot of staff had not logged in

We registered our own 2FA, logged into a Citrix desktop

Username enumeration

FOCA says “jbloggs” / “joe.bloggs”

- get lists of common firstnames, surnames and build yourself a target list

FOCA says U01234567

- try a few ranges near to the UIDs you find.

FOCA says jbl743

- you might be out of luck ; search space is too big and too sparse

Third example - TORU.com

Open URL redirect in holiday booking app

[THANK YOU SIMON]

Had already guessed two creds but needed more privs

Hosted a cloned page, but with “wrong password” error

The phishing email gave a legitimate page with ?url=phish

```
https://pto.toru.com/login?url=https://pto-toru.com/phishing
```

“we’ve lost some recent holiday bookings, please check”

TORU

Users would get “[EXTERNAL]” in the Subject line

BUT the link was obviously to their own site

The real site: took username & password – redirect to phishing page on SUCCESS

The phish site: “wrong creds, retry” – redirects back to a **valid logged in session**

No-one even noticed they’d been phished

Let’s see that step by step if we’ve got time

ASUS Router Example; long since fixed

Same mechanics but without mentioning actual client.

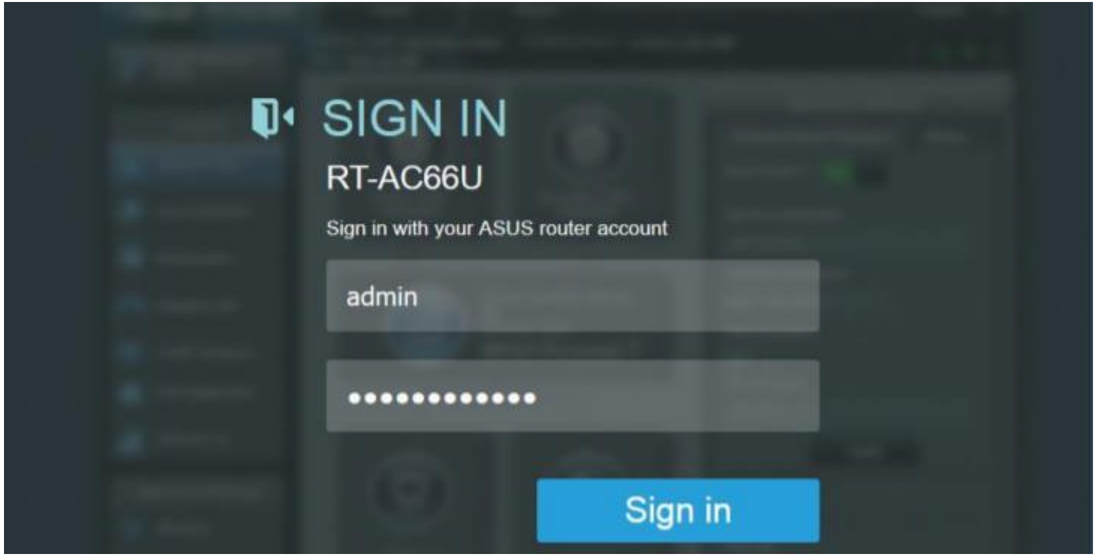
“Please update the firmware on your ASUS router ! Visit http://router.asus.com/Main_Login.asp?page=//router-asus.com/ and press ‘Check’ to check for the updated firmware.”

(ASUS router resolves “router.asus.com” to 192.168.1.1)

ASUS router – the real page

Genuine page loaded from phishing link, at

router DOT asus.com



SIGN IN

RT-AC66U

Sign in with your ASUS router account

admin

•••••••••••••

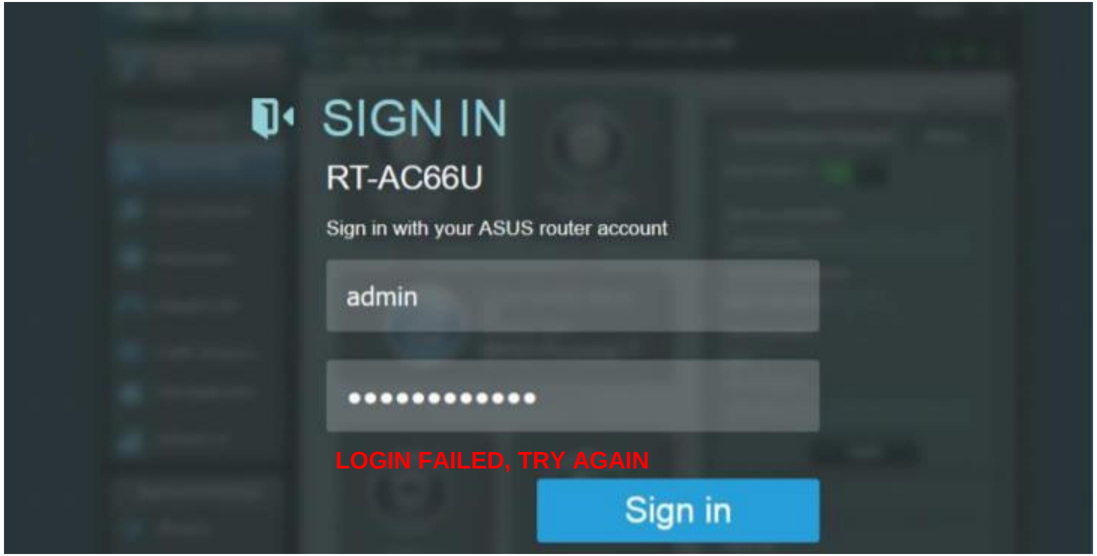
Our Phishing Page

Upon successful login, redirects to fake ?page= at our phishing site

router DASH asus

We log the input

Redirect back



SIGN IN

RT-AC66U

Sign in with your ASUS router account

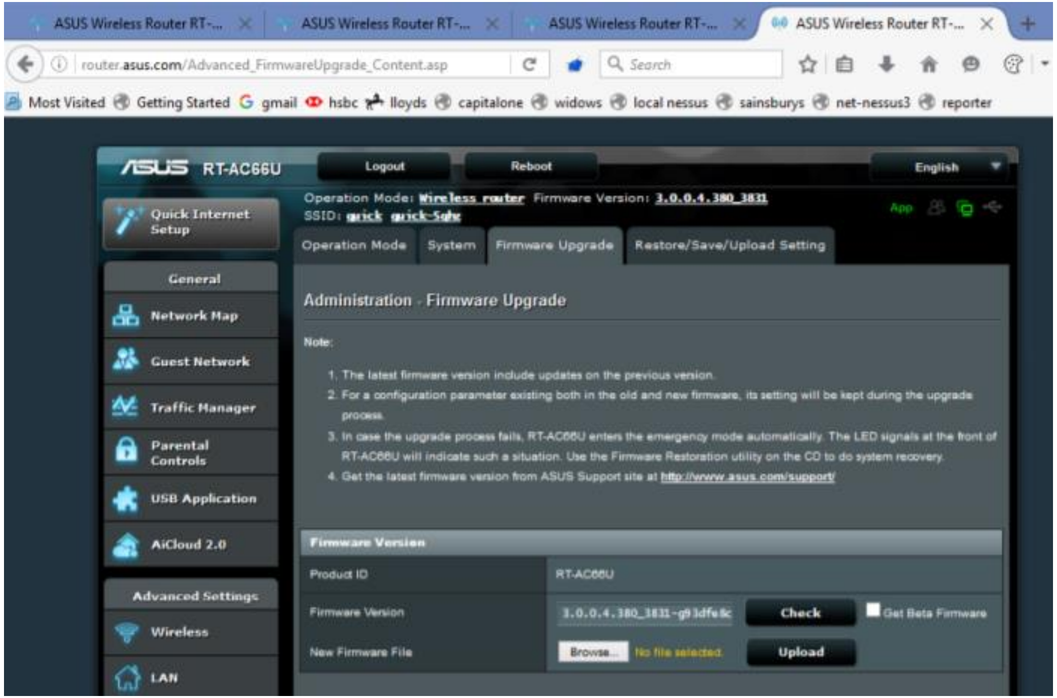
admin

•••••••••••••

LOGIN FAILED, TRY AGAIN

Redirect back to valid session

We log creds, victim gets redirected back into a valid session on the real server, none the wiser.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.380_3831
SSID: quick quick-5ghz

Administration - Firmware Upgrade

Note:

1. The latest firmware version include updates on the previous version.
2. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.
3. In case the upgrade process fails, RT-AC66U enters the emergency mode automatically. The LED signals at the front of RT-AC66U will indicate such a situation. Use the Firmware Restoration utility on the CD to do system recovery.
4. Get the latest firmware version from ASUS Support site at http://www.asus.com/support/

Firmware Version

Product ID: RT-AC66U

Firmware Version: 3.0.0.4.380_3831-g93dfe8c □ Get Beta Firmware

New Firmware File: No file selected.

TORU

IT used a domain squatting service and blocked our URL on the corp proxy

But - middle of COVID so everyone was home

Also, a MAJOR holiday was coming up

We got about 12 sets of valid creds out of this,

(including some remote access)

No one even knew they'd been phished

Fourth example - RIMA.com

Hybrid AD – so again, password spraying against MSOL

User IDs were numeric again, “U01234567”

Found a few passwords, again MonthYear or SeasonYear!

Oh no, everything is 2FA.

Except for ActiveSync mail protocol (cf MFASweep)

Use Windows 10 Mail to send email from compromised user to another user

Tools: MFASweep

Once you are have valid creds, MFASweep will

- try a bunch of MSOL services to see whether 2FA is in use
- suggest tools to exploit anything found
- lock the account out if you were wrong about the creds

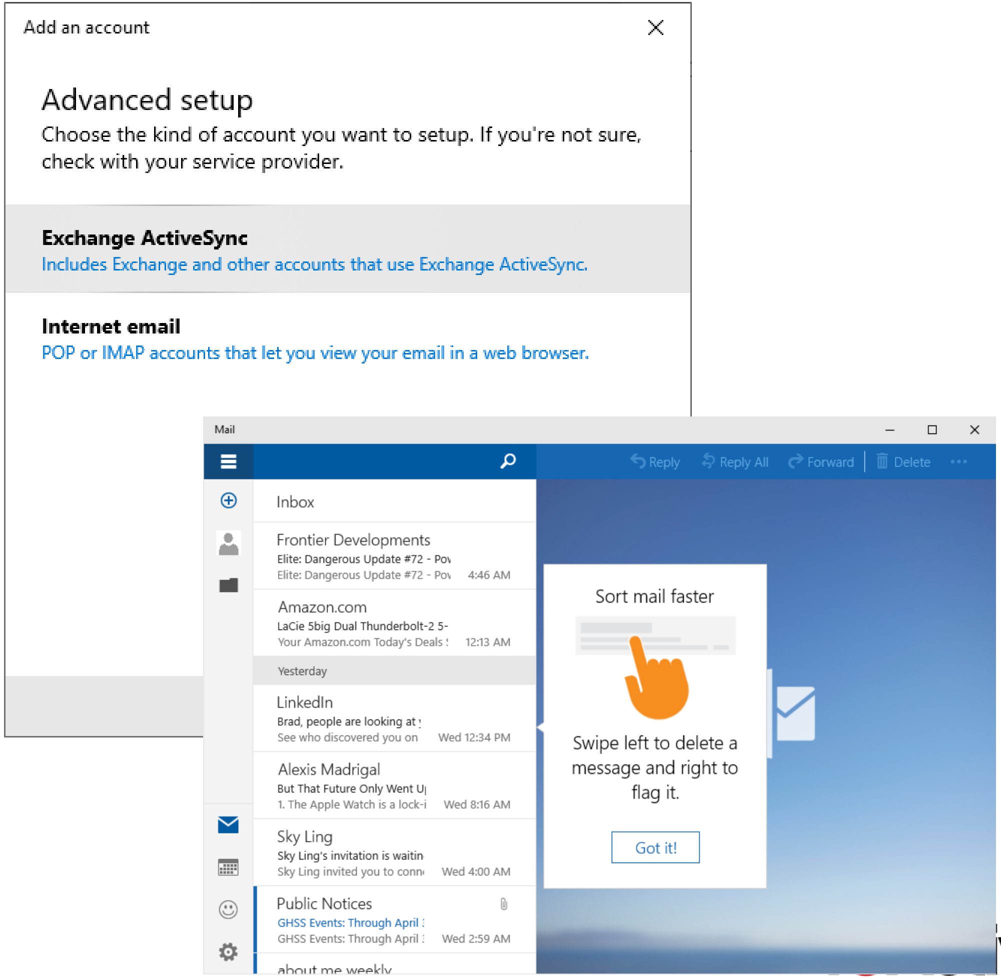
MFA login might text someone, so be careful probing web logins

RIMA & Windows Mail

Filtering between internal mailboxes is less aggressive

Find a recent mail, reply to it and attach your custom implant

“Can you open this?”



Add an account

Advanced setup

Choose the kind of account you want to setup. If you're not sure, check with your service provider.

Exchange ActiveSync
Includes Exchange and other accounts that use Exchange ActiveSync.

Internet email
POP or IMAP accounts that let you view your email in a web browser.

Frontier Developments
Elite: Dangerous Update #72 - Pov
Elite: Dangerous Update #72 - Pov 4:46 AM

Amazon.com
LaCie 5big Dual Thunderbolt-2 5-
Your Amazon.com Today's Deals : 12:13 AM

Yesterday

LinkedIn
Brad, people are looking at y
See who discovered you on Wed 12:34 PM

Alexis Madrigal
But That Future Only Went U|
1. The Apple Watch is a lock-i Wed 8:16 AM

Sky Ling
Sky Ling's invitation is waitin
Sky Ling invited you to conn Wed 4:00 AM

Public Notices
GHSS Events: Through April :
GHSS Events: Through April : Wed 2:59 AM

about me weekly

Sort mail faster

Swipe left to delete a message and right to flag it.

“Defenders think in lists, attackers think in graphs”

A path through a graph is obvious in hindsight

Actually generating a path involves trial and error, and backtracking

(breadth-first search)

To stretch and analogy much too far, pause and admire the view for a minute

We just got code exec inside the perimeter, from zero

So …

A combination of “minor” issues can be very serious

User enumeration exists in a lot of different places

Password spraying is a numbers game, so >1k valid users

Persevere if your first tries don’t work.

Bigger companies can be easier – more surface area

Monitor everything. Log everything. Yes, in the cloud too.

Weak passwords need to be changed proactively.

Test your own stuff; someone else probably is already

Questions?

Tools: Spraying Toolkit, MailSniper, MFASweep
Selenium, Chrome, LyncSniper, MSOLSpray.py

References

https://github.com/byt3bl33d3r/SprayingToolkit

https://github.com/dafthack/MailSniper

https://github.com/dafthack/MFASweep

https://blog.procircular.com/writing-custom-password-sprayers-with-selenium

https://github.com/mdsecresearch/LyncSniper

https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/

Incomplete and in no particular order; Tech people I owe :

JOE H

MATT T

SIMON

PETE

TAU

MARIO

ALEX B

RKL

IOA

DAVE L

MARIE

GLENN

CHRIS W

NICK F

GRANT

GHOSTIE

GEOFF

TAKESHI

JOHN O’

KEITH

LUKE T

OLIVER

KTT

DAVE F

WOODY

RICH W

PETER G

NICK R

ROY B

DAVE L

SENAD

ANDREW

LAURENT

HN/P