SECURITY (COMP0141): AUTHENTICATION ATTACKS

A RECENT PHISHING EMAIL

Metropolitan Police uk <d.j.ashley@comcast.net>

Dear Beneficiary;

My name is Inspector William Park, am working as the Head of Investigation with METROPOLITAN POLICE DEPARTMENT. there is presently a counter claims on your funds by one MR. BRENT STEVEN, who is presently trying to make us believe that you are dead and even explained that you entered into an agreement with him before your death, to help you in receiving your fund US$10,500,000.00 So here comes the big question.
Did you sign any Deed of Assignment in favor of (BRENT STEVEN), He further claimed that you died on the 9/MARCH/2019 and you have been buried, thereby making him the current beneficiary with his following account details:

ACCOUNT NAME: BRENT STEVEN
AC/NUMBER: 63758742.
ROUTING NUMBER: 122006743,
BANK NAME : FIRST BANK OF AMERICA
ADDRESS: NEW YORK, USA,

We shall proceed to issue all payments details to the said Mr. Brent Steven, if we do not hear from you within the next two working days from today. Are you truly dead as it was claimed by Mr. Brent Steven. You should also provide us with your direct telephone number where we can reach you today and what time we can get you on telephone.

If you are still alive you should contact the bank immediately.
Reply back ASAP.

Best Regards
Inspector Mike Lucas

PHISHING

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

We already saw phishing when we looked at scams in Week 5

PHISHING AND FRIENDS

Phishing happens via email

Vishing happens over the phone (“voice phishing”) - can use deepfake techniques to perform impersonation

Smishing happens via SMS

Pharming is a technique to enhance phishing

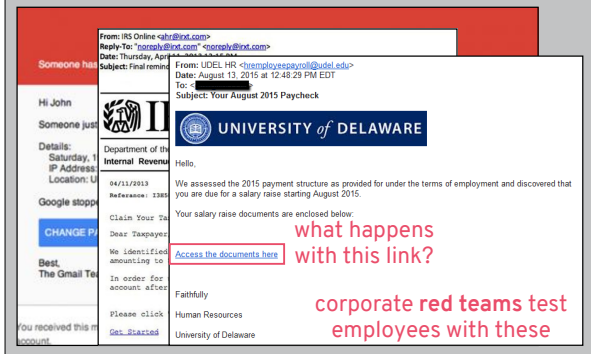
We’ll see what pharming is in just a few slides

PHISHING

5

This is a very simple phishing email, relatively easy to realise what's going on

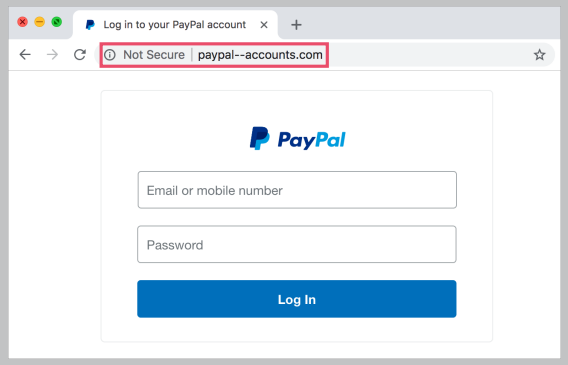
SPEAR-PHISHING



6

Spear-phishing emails are more targeted, so it's much easier to get users to click on these links. What actually happens once they do?

A PHISHING WEBSITE



7

Phishing websites almost always involve getting you to enter your password (or occasionally other sensitive information). They look normal so the only clue users have is in the address bar

WRONG URLS/TYPOSQUATTING

http://www.secure-trustedbank.com/

http://www.trustedbank.com@evilsite.com/

http://www.trustedbank.com@72.167.76.127/

https://www.trustedbank.com.in/

irrelevant if attacker owns domain!

http://www.steamcomrnunity.com/

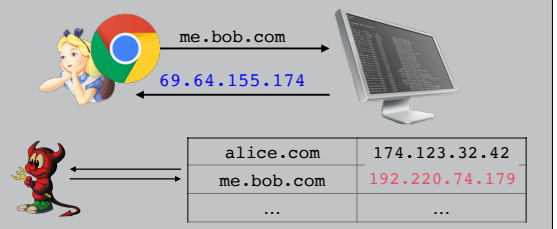
http://www.lioydsbank.com/

also used for other nefarious purposes (drive-by downloads, ad revenue, etc.)

8

The @ sign in a URL takes you to the second site, regardless of what comes before it. So even though some of these sites might appear normal if you glance at them, they can all be owned by adversary. Doesn't matter if they have the padlock because it's the attacker who is the legitimate owner of the domain

PHARMING



9

Pharming is very hard to do anything about, since the URL in the address bar is actually the right one so everything looks right. It is an example of a general issue called DNS spoofing that we'll explore in Week 9

OTHER ATTACKS ON 'WHAT YOU KNOW'

Capture attacks:

- Skimming (works for PINs)
- Keylogging
- Packet sniffing (unencrypted web traffic)

Intimate partner violence (attacker doesn't need to guess)

Observation attacks (shoulder-surfing)

Side-channel attacks (keyboard emanations, finger grease)

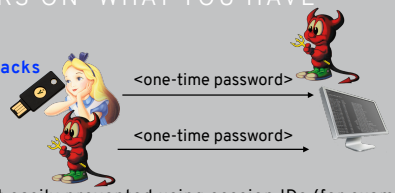
Coercion ("rubber-hose") attacks

10

We already saw some of these: keylogging in Week 5, packet sniffing in Week 3, IPV in Week 6, and side-channel attacks in Week 3

ATTACKS ON 'WHAT YOU HAVE'

Replay attacks

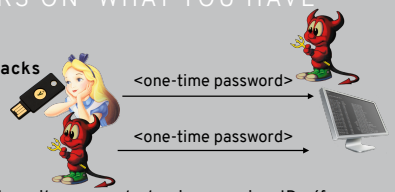


Classic but easily prevented using session IDs (for example)

Replay attacks are classic (not just for authentication!) but easily prevented by sensible implementation choices (https://en.wikipedia.org/wiki/Replay_attack)

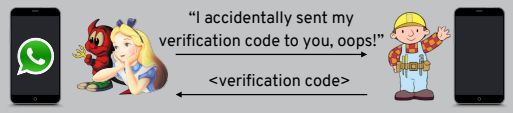
ATTACKS ON 'WHAT YOU HAVE'

Replay attacks



Classic but easily prevented using session IDs (for example)

Verification scams

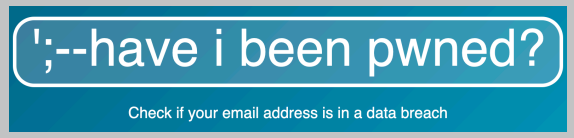


...registers Bob's number...

...gets verification SMS...

Verification scams are another type of social engineering attack, which makes them harder to prevent

HAVE I BEEN PWNED? (DEMO)



Can check if your password is part of one of these frequent breaches by checking https://haveibeenpwned.com/

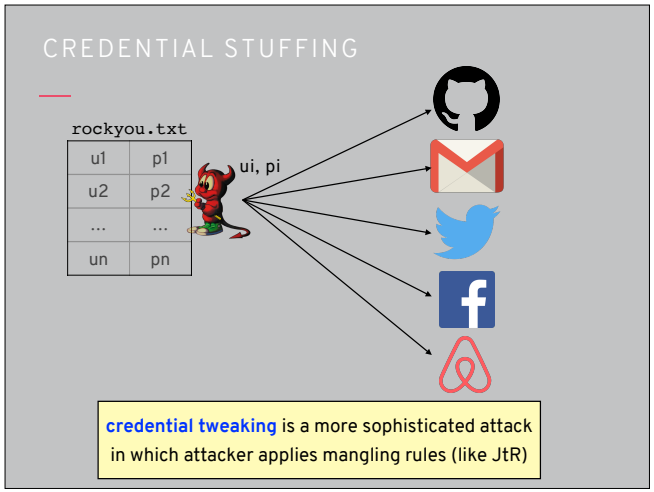
PASSWORD REUSE

If your Hotmail password is compromised, this has obvious implications for your Hotmail account security

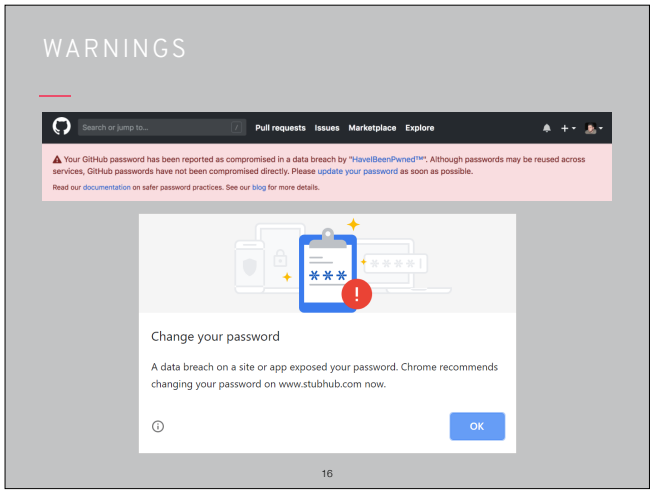
What about your Github account? Gmail?

How many different accounts do you have (N)? How many different passwords (M)? Is N ≫ M? 👀

Data breaches on a single platform also seriously affect other platforms because of password reuse



A credential stuffing attack exploits password reuse to try guessing compromised passwords on uncompromised sites. There are very few capabilities required – the attacker can even just do this manually



Some platforms now warn their users about breaches that involve a reused password

SOLUTIONS

Password cracking is an **offline** **guessing attack**: have as many guesses as your hardware/patience allows

Credential stuffing is an **online** **guessing attack**: have as many guesses as the platform allows before locking account

- Too permissive? Higher risk of the attacker succeeding
- Too strict? Higher risk of the (real) user getting locked out

Can limit number of guesses to reduce effectiveness of an online guessing attack

PASSWORD REUSE

If your Hotmail password is compromised, this has obvious implications for your Hotmail account security

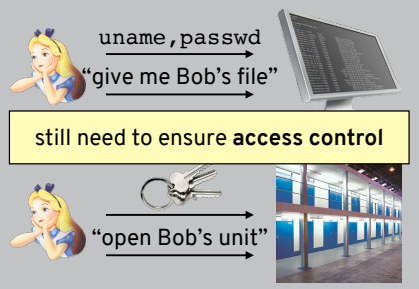
What about your Github account? Gmail?

How many different accounts do you have (N)? How many different passwords (M)? Is N ≫ M? 👀

Password managers ensure that N = M
(but have their own set of issues!)

Can also try to make sure each user has a unique password for every account – achievable using password managers, although these come with usability and security issues of their own (for example they serve as a single point of failure)

ACCESS CONTROL



Next week we’ll focus on the topic of access control

QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2833302`

to take this week’s quiz!