FACULTY OF SCIENCE & TECHNOLOGY
Department of Computing & Informatics
Forensic Computing & Security

Enterprise Security & Privacy

Paul-David Jarvis
s5115232@bournemouth.ac.uk

Security & Privacy in the financial service industry

Table of Contents

List of Figures

List of Tables

1.0 Technical Analysis

1.1 Introduction

1.1.1 Scope & Context

Banks and banking credentials are a huge target for threat actors. Especially opportunists, terrorists and cold intellectual attackers. The credentials themselves can be used to log into the victim's bank account and cipher their money or even to be sold on the dark web or just leaked online. There are tons of online databases that hold this leaked information such as the database known as "Collection #1" through to "Collection #5" that affects as many as 770 million people and includes more than 20 million passwords in plain text (Brewster, 2019). A very popular and successful banking trojan is Emotet.

All my dumps are HIGH BALANCE!!!! 1 DUMP = 10 CC Fullz

Fullz info Format is:

|Card Number|EXP. Date|CVV2|First Name|Last Name|Address|City|Zipcode|State|Country|Phone number|SSN|DOB|Mother's Maiden Name|Social Security Number|

Will send dumps to you immediately after we receive your payment for the order

I always replace bad, declined dumps

Replacement of invalid dumps can be made within 24 hours

==> Card Dumps from Us : (101) (201)

===> Price for Dumps:

- Visa Classic|Master Standard = 150$ ($5,000+ Balance)
- Visa|Master|Amex|Discover (Gold,Platinum) = 225$ ($10,000+ Balance)
- (Business,Signature,Purchase,Corporate,Travel) = $480 ($20,000+ Balance)

Figure 1. Dark Web Advert

1.1.2 Security Attack

Emotet is a banking trojan that targets anyone. It has targeted individuals, companies and governments worldwide. Emotet can come in various file formats and attached to spam emails. Once infected, the trojan will send itself to everyone it can. It can also spread by brute forcing other devices connected on the network. Emotet would steal user's credentials by eavesdropping and saving outgoing network traffic. The impact is huge for whoever is infected. It's not only the victims bank accounts that are targeted but everything else. Allentown in Pennsylvania reportedly cost the city upwards of a million dollars when they requested Microsoft's incident response team to help clean it up. Emotet has a polymorphic nature which causes issues when trying to contain it.

1.1.3 Privacy Attack

Credential stuffing is a technique used by attackers to gain access to accounts. The attackers target victims of personal data leak such as Collection #1. The attackers would acquire the credentials from data dumps and brute force into sites like their social media, online marketplaces and banking sites (Owasp.org, 2018). Leaked personal data is in breach of the GDPR Principle 7; stating that personal information should be kept securely and confidential. The impact on these victims are huge, their data are sold, leaked or used for malicious purposes. Lance Miller who was wrongfully arrested because his wallet was stolen and was impersonated. His bank accounts were drained, and credit cards maxed (Krebsonsecurity.com, 2016). HSBC had a data breach. Credential stuffing was used to gain access to stolen accounts and customers' names, addresses, phone numbers, email addresses, account numbers and balances, transaction history and account information of their payees were leaked (Titcomb, 2018). This information is classed as personal data and can be used to identify a person. HSBC had an obligation to keep this data confidential and safe. There is no definite way to stop data breaches. Which is why credential stuffing is an emerging attack. Attackers will always find new ways to exploit software and sell classified data. Sometimes it's not always an outsider. A former swiss banker named Rudolf Elmer who passed data of 2,000 prominent people to Julian Assange, the owner of Wikileaks (BBC News, 2011).

1.2 Proposed Solutions

1.2.1 Listing of different solutions or tools or apps or software security

Malwarebytes released an article on Emotet stating that their software can detect and quarantine Emotet. They also published several suggestions on how to remove Emotet on networked machines more effectively due to the nature of the trojan; they suggested that you first identify the infected machines, secondly you disconnect the infected machine from the network. Thirdly you install the patch for Eternal Blue. Lastly you disable administrative shares and can safely remove the Emotet trojan and change the account credentials (Malwarebytes Labs, n.d.).

F5 Labs released an article about Emotet and suggestions on protecting yourself against it. Multi-factor authentication whenever possible is suggested. Using a password manager is also suggested, trojans carry keyloggers so using a password manager will store your credentials. Double checking websites before entering any credentials to spot a fake website is also suggested. (Cohen and Walkowski, 2019). SocialFish was used and allowed me to duplicate PayPal and capture credentials, shown in figure 2.

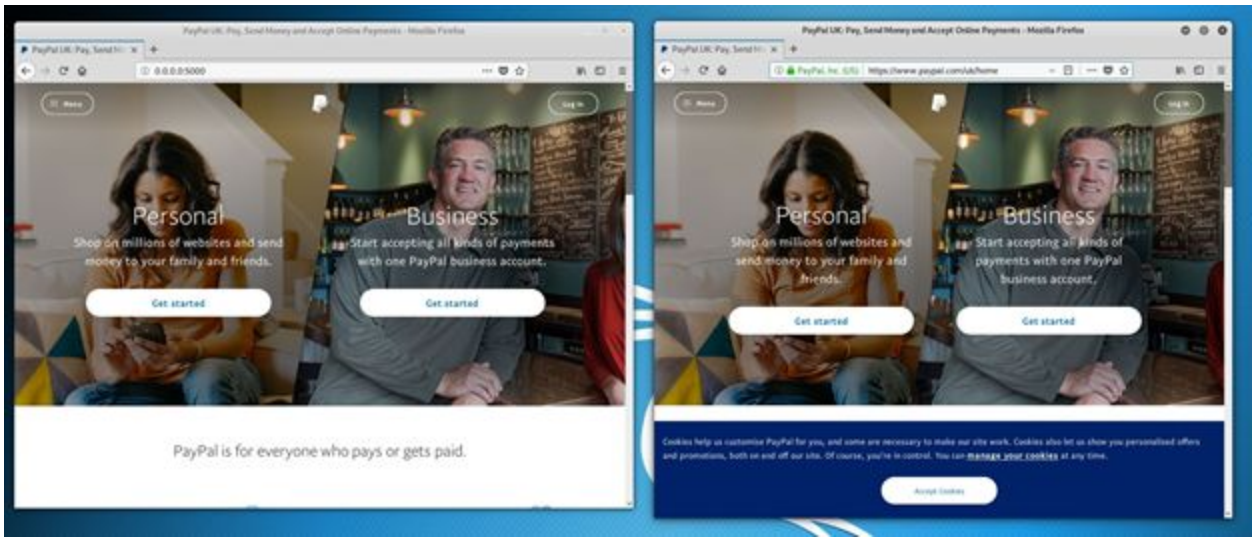

Figure 2. Real & Fake PayPal

Figure 3 and 4 are data packets that were captured when I entered credentials at my fake website. These credentials were captured in plaintext. Malicious actors would use tools like SocialFish and spoof the URL into something similar to tools like dnstwist. Dnstwist is shown in figure 5.

'/login', 'forcePhonePasswordOptIn': '', 'login_email': 'test123@hotmail.com', 'splitLoginContext': 'inputEmail', '_sessionID': 'null'}

Figure 3. Plaintext Email

'forcePhonePasswordOptIn': '', 'login_email': 'testpassword', '_sessionID': 'null'}

Figure 4. Plaintext Password

Figure 5. Dnstwist

Learning how to spot potential phishing emails and not to click on suspicious links included in the email is also suggested. This is the main method of spreading trojans and malware. Figure 6 is an email from someone pretending to be the Bank of America in order to phish credentials.

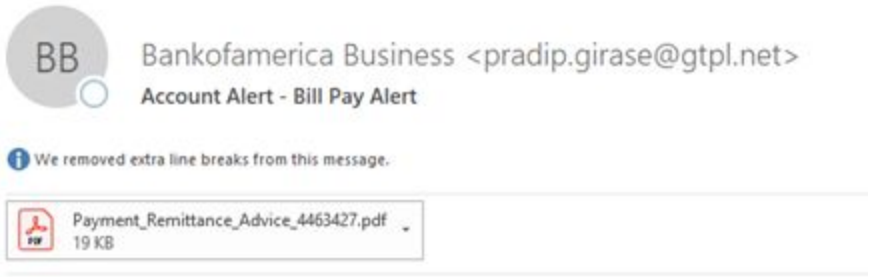

Figure 6. Phishing Email

1.3 Privacy

Which released an article to help victims of personal data leaks. The first suggestion is to change your password (Which? Consumer Rights, n.d.). Collection #1 holds 2.7 billion records and

773 million email addresses. “haveIbeenpwned?” can be used, your email address is entered, and it will let you know whether you have been a victim. This is shown in both figures 7 and 8.

Figure 7. HaveIBeenPwned?

Figure 8. Collection #1

1password is a password manager that will help you keep your privacy. It allocates passwords to your accounts which protects you if one of them has been breached. It features a two-factor authentication and will alert you as soon as one of your accounts have been compromised (1Password, 2019).

Virtual Private Network (VPN) is another suggestion. VPNs use encryption technology and protocols, such as Layer 2 Tunneling Protocol (L2TP), Secure Socket Layer (SSL) and Transport Layer Security (TLS). This creates a “tunnel” between you and the VPN server and is completely secure and private (Vaughan-Nichols, 2018).

Mashable released an article about Hypertext Transfer Protocol Secure (HTTPS) and suggested that you enter your details on a secure site only. It creates a secure connection and stops attackers from eavesdropping. (Shema, 2011). Figures 9 and 10 show two intercepted packets from a secure site and not a secure site.

Figure 9. Encoded Packet

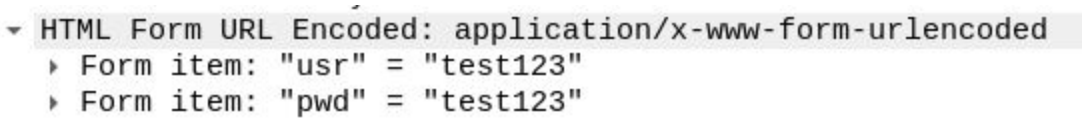

Figure 10. Plaintext Packet

1.4 Security & Privacy Attack Solutions Comparison

Security Attack Solutions	
Attack Solution	**Comparison**
MalwareBytes or any fundamental protection.	Antivirus will immediately detect a fake website that contains anything malicious. Outlook includes their own spam filter that filters phishing emails.
Multi-factor Authentication.	MFA is another layer of security and having it enabled is good practice. Some may argue that this isn't as important as having an antivirus but ideally you should have both. It doesn't protect you in the way that Malwarebytes would.
Password Manager.	They store your credentials, saving you from remembering them or writing them down. SImilar to MFA, it doesn't protect you as much as anti-virus.
Checking the website for anything suspicious or fake.	Knowing what to look for is extremely useful, it will stop you from entering credentials on a fake website. Fundamental protection like malwarebytes will do this automatically however.
Learning to spot fake emails and spam links.	Knowing common fake emails will protect you from downloading malware that is spread through spam links and phishing emails.

Table 1: Security Attack Solutions

Privacy Attack Solutions	
Privacy Solution	**Comparison**
Changing Passwords.	You should change your password regularly. Having unique passwords such as the ones that 1password allocates will reduce the need for you to change them.
Haveibeenpwned?	Websites like “haveibeenpwned?” are great. They let you know whether any of your personal information have been leaked in massive collections. This is an integrated function in their password manager they released.
1password.	1password manager is a great piece of software, it features tons of functions like allocating unique passwords and letting you know whether they’ve been compromised.
VPN.	VPNs are a great solution to keep your privacy intact. Especially in areas with free wifi like a coffee store where they’re prime targets for threat actors.
HTTPS.	Stops malicious threats from eavesdropping and intercepting personal data. A VPN is similar and both encrypts your data. ISP’ can only see that you’re connected to a VPN server. Using a HTTPS website then they can only see what site you’re connecting to (NordVPN, 2019).

Table 2: Privacy Attack Solutions

1.4 Best Solutions

1.4.1 Security

The best solution(s) to protect yourself from a security attack is having MalwareBytes or any antivirus installed. It will alert you if you try to enter any malicious websites and block malicious downloads. Multi-factor authentication should also be used. Having a password manager is also suggested.

1.4.2 Privacy

The best solution(s) to protect your privacy is encrypting your traffic data by using secure websites or a VPN. This stops attackers from intercepting information such as your bank account number, credentials and any other identifiable information under the GDPR. Checking credentials for leaking using websites like haveibeenpwned. This is sometimes integrated into a password manager like 1password. This ensures that your credentials can not be compromised as well as alerting you when your credentials have been compromised and storing and allocating long and complex passwords to the websites you use daily.

2.0 Reflective Analysis

2.1 Group Work Personal Strengths & Weaknesses

I believed during the group work I took a leader position. I was extremely organised and I knew what everyone was doing and what their roles were, this allowed me to plan the poster more efficiently, so we didn't have to repeat information and knew what we were putting in the sections on the poster. I created a document in which we planned the individual report and poster, in this report I went through every official document given to us and extracted the important information to make it easier on my team. I coordinated everyone and got together, I wrote the emails and got everyone in contact with each other through Facebook. This allowed us to all meet at 1:00PM and talk about what we are doing.

I believe the main weakness during the group work was my lack of understanding the assignment brief. My group asked me several questions when we met up and wanted me to clarify what the brief was saying, however because I wasn’t sure myself, I couldn’t answer the

questions that my group was throwing at me and I felt like not being able to answer their questions was letting the group down and them down.

2.2 Group Work Strengths & Weaknesses

My group were extremely enthusiastic and eager to meet and talk about the poster and our presentation. I believe that we were communicating with each other efficiently and that allowed us to talk about what we should include in the sections of the poster and if we had any questions or problems then everyone felt safe to ask them.

I believe that our entire group had the same weaknesses. We had issues at the start as we struggled to understand the assignment brief and wasn't entirely sure on a few examples such as the "application for consumers" and what the brief meant by tools when it stated in the poster example "impact and use of the developed tool".

2.3 What Did I learn?

I learnt several things when researching for this assignment. I researched in detail security and privacy solutions and learned about loads of open source tools for Kali and how threat actors could use these online tools to breach security and privacy for banks and users. I was able to apply the theory I have learnt to practice by installing these tools and using them as threat actors and malicious hackers would. I saw how easy it is to clone a popular website such as PayPal and online banking like Tesco using the tool SocialFish and to check the thousands of potential different but similar domains that users don't notice using DNSTwist.

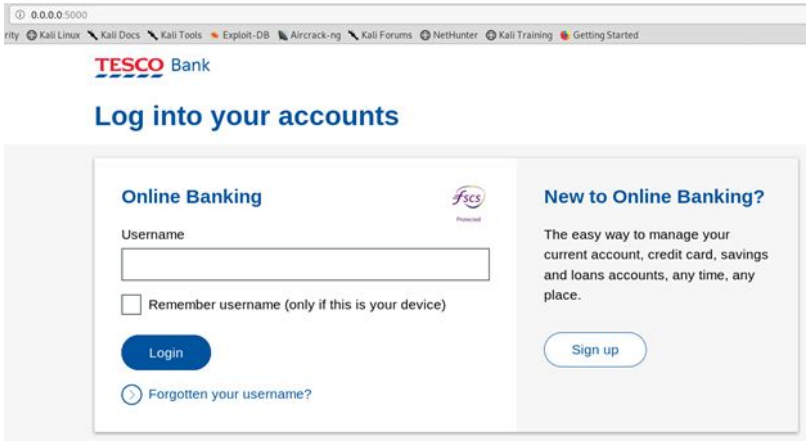

Figure 11: Fake Tesco Banking

Figure 12. Dnstwist

2.4 What Would I do differently Next Time?

When I was writing this, I was very unsure if what I was writing was correct because I was unsure, I didn't want to ask because I felt like a big part of this assignment was researching. If I was to do something differently next time, it would be to talk to someone for clarification.

References

Brewster, T. (2019). *Hackers Behind A 770 Million Mega Leak Are Selling 10 Times More Data -- But Don't Panic*. [online] Forbes.com. Available at: https://www.forbes.com/sites/thomasbrewster/2019/01/21/hackers-who-leaked-collection-1-are-selling-10-times-more-data-but-you-dont-need-to-panic/#2019ea6a7c15 [Accessed 10 Oct. 2019].

BBC News. (2011). *Wikileaks given Swiss bank data*. [online] Available at: https://www.bbc.co.uk/news/business-12205690 [Accessed 11 Oct. 2019].

Krebsonsecurity.com. (2016). *From Stolen Wallet to ID Theft, Wrongful Arrest — Krebs on Security*. [online] Available at: https://krebsonsecurity.com/2016/03/from-stolen-wallet-to-id-theft-wrongful-arrest/ [Accessed 11 Oct. 2019].

Owasp.org. (2018). *Credential stuffing - OWASP*. [online] Available at: https://www.owasp.org/index.php/Credential_stuffing [Accessed 11 Oct. 2019].

Titcomb, J. (2018). *HSBC suffers data breach at US bank*. [online] The Telegraph. Available at: https://www.telegraph.co.uk/technology/2018/11/06/hsbc-suffers-data-breach-us-bank/ [Accessed 11 Oct. 2019].

Malwarebytes Labs. (n.d.). *Trojan.Emotet - Malwarebytes Labs*. [online] Available at: https://blog.malwarebytes.com/detections/trojan-emotet/ [Accessed 10 Oct. 2019].

Cohen, R. and Walkowski, D. (2019). *Banking Trojans: A Reference Guide to the Malware Family Tree*. [online] F5 Labs. Available at: https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree [Accessed 10 Oct. 2019].

Research, E. (2018). *Emotet launches major new spam campaign | WeLiveSecurity*. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/ [Accessed 10 Oct. 2019].

Which? Consumer Rights. (n.d.). *My data has been lost after a breach, what are my rights?*. [online] Available at: https://www.which.co.uk/consumer-rights/advice/my-data-has-been-lost-what-are-my-rights [Accessed 11 Oct. 2019].

Have I Been Pwned: Check if your email has been compromised in a data breach. (2013). *';--have i been pwned?*. [online] Available at: https://haveibeenpwned.com [Accessed 10 Oct. 2019].

1Password. (2019). *1Password loves Have I Been Pwned | 1Password*. [online] Available at: https://1password.com/haveibeenpwned/ohno/ [Accessed 11 Oct. 2019].

Vaughan-Nichols, S. (2018). *How to use a VPN to protect your internet privacy | ZDNet*. [online] ZDNet. Available at: https://www.zdnet.com/article/how-to-use-a-vpn-to-protect-your-internet-privacy/ [Accessed 11 Oct. 2019].

Shema, M. (2011). *Web Security: Why You Should Always Use HTTPS*. [online] Mashable. Available at: https://mashable.com/2011/05/31/https-web-security/?europe=true [Accessed 11 Oct. 2019].

NordVPN. (2019). *HTTPS vs. VPN: Why you need both*. [online] Available at: https://nordvpn.com/blog/https-vs-vpn/ [Accessed 11 Oct. 2019].