Information Gathering

Preliminary Technical and Adversarial Information Gathering on JP Morgan Chase

Prepared by: Isabelle Jaber

Date: August 5th, 2024

Table of Contents:

EXECUTIVE SUMMARY

In this information-gathering exercise, publicly available information was leveraged to gain a basic understanding of what information could be found regarding JP Morgan Chase's tech infrastructure. In addition, an examination of their social media, relevant news articles, and anonymous professional forums gave insight into potential motivations customers or employees may have to launch a cyber attack against the company.

To do this, simple commands in the terminal were used to see what IP addresses could be found associated with the jpmorganchase.com domain. This information was then passed to online tools including Shodan and WHOIS. Further research was done on various news outlets to determine if there was any information that would be relevant to JP Morgan Chase customers and/or employees. Further research on their public image/engagement was done on X (formerly known as Twitter) and Instagram.

These investigations revealed that information on encryption methods, SSL certificates, and host names are all publicly available, and could be found just by checking one IP address associated with JP Morgan Chase's domain. Additionally, JP Morgan Chase lacks customer engagement via their social media platforms, and their resistance to protecting their customers who are scammed or are victims of fraud does not align with how they advertise themselves. Finally, through investigations on TeamBlind, it was determined that JP Morgan Chase is not rated very highly in terms of compensation and benefits by its employees. The technical data collected may provide a focus for risk mitigation, while the data surrounding JP Morgan Chase's public relations may indicate potential motivations for an attack thereby providing the security team with the information required to properly prioritize the company's assets.

INTRODUCTION

Project Background

This report will provide information (within the defined scope) on JP Morgan Chase. JP Morgan Chase is an American multinational banking and financial services holding company that has been "built on the foundation of more than 1,200 predecessor institutions that have come together over the last 225 years to form today's company" (JP Morgan Chase History Page.) The company evolved from The Manhattan Company, The New York Clearing House, The New York Guaranty and Indemnity Company, Bank One, Drexel, Harjes & Co., Drexel, Morgan & Co., Chase National Bank, First National Bank of Chicago, Brooklyn Trust Company, J.P. Morgan & Co., Equitable Trust Company, and many more. Now their business principles include exceptional client services, operational excellence, a commitment to integrity, fairness, and responsibility, and a great team and winning culture.

According to Craft Co. JP Morgan Chase's competitors include Morgan Stanely, HSBC Holdings, Citigroup, Wells Fargo, and Bank of America. Out of these competitors, JP Morgan Chase has the most employees (311,921), the highest valuation ($571.9 billion), the highest estimated revenue ($239.4 billion), the highest gross profit ($158.1 billion), and the highest net income ($49.6 billion). JP Morgan Chase has received the following awards:

- Firmwide Impact Awards:
  - JPMorgan Chase named in LinkedIn's 2024 Top Companies list
  - FORTUNE names JPMorgan Chase the 5th Most Admired Company in the World (2024)
  - TIME100 Most Influential Companies (2023)
  - 2023 Fortune Change the World
- DEI Awards:
  - Forbes names JPMorgan Chase one of the Best Employers for Diversity (2020-2024)
  - DiversityComm Magazine recognizes JPMorganChase as a Top Black Employer (2024)
  - DiversityComm Magazine recognizes JPMorganChase as a Top Hispanic Employer (2024)
- HR and Talent Awards:
  - JPMorgan Chase ranked #1 on Universum's list of Most Attractive Employers in the U.K. and in Singapore (2024)
  - JPMorgan Chase named in LinkedIn's 2024 Top Companies list

  - JPMorgan Chase wins 2024 Handshake Early Talent Award and named Tech Transformer
  - Business Group on Health names JPMorganChase a 2024 Best Employers: Excellence in Health & Well-being Award winner
- Tech Awards:
  - JPMorgan Chase wins 2024 Handshake Early Talent Award and named Tech Transformer
  - Handshake's 2023 Early Talent Awards names JPMorgan Chase a top employer and Tech Transformer

The Chairman and Chief Executive Officer (CEO) is Jamie Dimon. He has an MBA from Harvard University and has worked for American Express Company, Commercial Credit, Smith Barney Inc., and Citigroup Inc. He also serves on the boards of directors of the Business Roundtable, Bank Policy Institute, and Harvard Business School to name a few. Additionally, he serves on the executive committee of the Partnership for New York City and is a member of the Business Council, Financial Services Forum, and Council on Foreign Relations.

The Chief Financial Officer (CFO) is Jeremy Barnum. Since joining the firm in 1994, Jeremy has held several leadership roles at JP Morgan Chase including head of Global Research for J.P. Morgan's Corporate & Investment Bank (CIB), and Chief Financial Officer and Chief of Staff for the Corporate & Investment Bank. As CFO, Jeremy is responsible for Global Finance and Business Management, the Chief Administrative Office, the Treasury/Chief Investment Office, Control Management, and Business Resiliency.

The Chief Risk Officer (CRO) is Ashley Bacon. He has a degree in Monetary Economics from the London School of Economics. Throughout his career, he has traded international government bonds for Daiwa Securities and worked in JP Morgan Chase's Tokyo, Singapore, and London offices in a variety of trading roles. As the Chief Risk Officer, he is responsible for the Risk Management and Compliance organization across the Corporate & Investment Bank, Consumer & Community Banking, Asset & Wealth Management, Commercial Banking, and the firm's corporate activities.

The Global Chief Information Officer (CIO) is Lori Beer. As the CIO, she manages a $17 billion (USD) budget and more than 63,000 technologists supporting JPMorgan Chase's retail, wholesale, and asset and wealth management businesses. She holds a bachelor's degree in Computer Science from Dayton University and a Doctorate in Commercial Science from the University of Cincinnati. Before joining JP Morgan Chase she was the Executive Vice President of Specialty Businesses and Information Technology for WellPoint, Inc. She also serves as the sponsor of the firm's Women on the Move Business Resource Group. She has been named among the CIO 100 Hall of Fame, Forbes CIO Next list, Most Influential Women in US Finance by Barron's, the Most Powerful Women in Banking by American Banker, Top 3 Women in FinTech by FinTech Magazine, and a Merit Award recipient by the Women's Bond Club. Beer has also been recognized as a Computerworld Premier 100 IT Leader and National Association for Female Executives Women of Excellence Health Care Champion.

Scope and Objectives

The scope of this information-gathering initiative is to get a rudimentary understanding of how their public-facing websites are managed and examine how much information could be available for the wider network. This includes domain registration details, SSL certificate data, and encryption protocols. Another goal of this investigation is to use news articles and social media to understand their public relations and how recent actions have impacted potential threat actors and their motivations.

METHODOLOGY

Data Sources

- WHOIS: A public database that houses the information collected when someone registers a domain name or updates their DNS settings.
- Shodan: A search engine that lets users search for various types of servers connected to the internet using different filters
- DuckDuckGo: A search engine that, in this case, was used to search for relevant and current news articles, the JP Morgan Chase website, TeamBlind, and other resources used for this analysis.
- TeamBlind: Anonymous professional community forum. Used to gain insight into employees' experiences working for JP Morgan Chase.
- X (Twitter): Used to find their social media account and determine what kind of content they have been posting.
- Instagram: Used to find their social media account and determine what kind of content they have been posting.

Techniques Employed

An "nslookup" was performed on the "jpmorganchase.com" domain to get their IP address. This gave us the server, its address, and other non-authoritative IP addresses. The following query was then entered into the Shodan search engine using one of the on-authoritative IP addresses: "net: "159.53.34.8"". JP Morgan Chase's domain was passed to WHOIS to gather information on its domain and DNS settings. DuckDuckGo was the search engine used to find relevant news articles related to JP Morgan Chase. Research was conducted on X and Instagram to get a better understanding of JP Morgan Chase's social media engagement. TeamBlind was also used to gain a better understanding of how the employees experience the company culture. Various news articles were also accessed to get a better understanding of JP Morgan Chase's public image and public relations initiatives.

Ethical Considerations

Much of the technical data retrieved through the WHOIS analysis and Shodan could be used by attackers to exploit JP Morgan Chase's system. Even with just the details such as their DNS server, encryption methods, server names, and Extensible Provisioning Protocol (EPP) domain status codes, gathered from one IP address associated with JP Morgan Chase, attackers can gain extensive intelligence on JP Morgan Chase’s tech infrastructure. Since it is clear that this information is publicly available, this data can also be exploited by malicious actors.

Fortunately, WHOIS privacy services replace the domain owner’s contact information in the WHOIS database with their own. This shields the domain owner’s personal information from the public while still allowing for legitimate inquiries to be forwarded.

Global data privacy laws, such as the General Data Protection Regulation (GDPR) in Europe, are having a significant impact on WHOIS data. These laws impose strict rules and requirements on the collection, storage, and disclosure of personal data, including WHOIS data.

FINDINGS

WHOIS Analysis

- Domain: jpmorganchase.com.
- Registrar: MarkMonitor Inc.
- Registration created: 2000-09-12
- Registration expiry: 2025-09-12
- Registration updated: 2023-08-11
- Status:
  - clientDeleteProhibited
    - This status code tells your domain's registry to reject requests to delete the domain.
  - clientTransferProhibited
    - This status code tells your domain's registry to reject requests to transfer the domain from your current registrar to another.
  - clientUpdateProhibited
    - This status code tells your domain's registry to reject requests to update the domain.
  - serverDeleteProhibited
    - This status code prevents your domain from being deleted. It is an uncommon status that is usually enacted during legal disputes, at your request, or when a redemptionPeriod status is in place.
  - serverTransferProhibited
    - This status code prevents your domain from being transferred from your current registrar to another. It is an uncommon status that is usually enacted during legal or other disputes, at your request, or when a redemptionPeriod status is in place.
  - serverUpdateProhibited
    - This status code locks your domain preventing it from being updated. It is an uncommon status that is usually enacted during legal disputes, at your request, or when a redemptionPeriod status is in place.
- Name Servers:
  - ns0087.secondary.cloudflare.com
  - ns0134.secondary.cloudflare.com

  - ns05.jpmorganchase.com
  - ns06.jpmorganchase.com
  - ns1.jpmorganchase.com
  - ns2.jpmorganchase.com
- Registrant Contact, Administrative Contact, and Technical Contact:
  - Name: Domain Administrator
  - Organization: JPMorgan Chase & Co.
  - Street: 201 North Walnut Street, Mail Suite DE1-0175
  - City: Wilmington
  - State: DE
  - Postal Code: 19801
  - Country: US
  - Phone: +1.3022821773
  - Fax: +1.3022821660

Shodan Infrastructure Analysis

- Open Ports:
  - Port 80: Redirects unsecured HTTP traffic to a secure HTTPS protocol on port 443.
  - Port 443: Processes secure HTTPS traffic.
    - Expires: Sat, 03 Aug 2024 01:02:56 GMT
    - Location: https://www.jpmorgan.com/commercial-banking
    - SSL Certificate:
      - Validity
        - Not Before: May 3 06:00:34 2024 GMT
        - Not After: May 3 06:00:33 2025 GMT
      - Public Key Algorithm: rsaEncryption
      - Signature Algorithm: sha256WithRSAEncryption
- Hostnames
  - jpm.com
  - www.jpm.com
  - jpmc.co
  - jpmc.com
  - www.jpmc.com
  - jpmc.global

- jpmchase.com
- www.jpmchase.com
- www.jpmorgan.co.id
- www.jpmorgan.co.jp
- www.jpmorgan.co.kr
- jpmorgan.co.uk
- www.jpmorgan.co.uk
- jpmorgan.com
- cws-main.jpmorgan.com
- main-beta1.jpmorgan.com
- main-beta2.jpmorgan.com
- main-beta3.jpmorgan.com
- main-beta4.jpmorgan.com
- main-beta5.jpmorgan.com
- ordertopay.jpmorgan.com
- otp.jpmorgan.com
- query.jpmorgan.com
- www.jpmorgan.com
- jpmorgan.com.br
- www.jpmorgan.com.br
- jpmorgan.com.mx
- www.jpmorgan.com.mx
- www.jpmorgan.ru
- jpmorganchase.com
- about.jpmorganchase.com
- commercial.jpmorganchase.com
- impact.jpmorganchase.com
- institute.jpmorganchase.com
- ir.jpmorganchase.com
- news.jpmorganchase.com
- ordertopay.jpmorganchase.com
- otp-app.jpmorganchase.com
- otp-app-emea.jpmorganchase.com
- otp-csc.jpmorganchase.com
- otp-csc-https.jpmorganchase.com
- otp-csr-emea.jpmorganchase.com

- otp-csr-ro.jpmorganchase.com
- otp-emea.jpmorganchase.com
- otp-enrollment.jpmorganchase.com
- otp-jpm.jpmorganchase.com
- otp-nocsc.jpmorganchase.com
- otp-www.jpmorganchase.com
- query.jpmorganchase.com
- www.jpmorganchase.com
- jpmorganchase.page
- jpmorganchaseco.co
- www.jpmorganchina.com.cn
- jpmorgansecurities.com
- www.jpmorgansecurities.com
- xign.com
- xign.net
- app.xign.net
- app-emea.xign.net
- csr-emea.xign.net
- csr-ro.xign.net
- emea.xign.net
- www.xign.net
- xign.org

Social Media and News Insights

They appear to only post on X once quarterly since the beginning of 2024, while in 2023 they seemed to be posting a few times per month. Posts mostly consisted of advertisements, reading lists, and JP Morgan Chase research. All they have posted in 2024 have been quarterly reports and letters to shareholders. On Instagram, they haven't posted at all.

Recently, top headlines about JP Morgan Chase have been concerning scam reimbursements. Zelle is the leading U.S peer-to-peer payment network owned by seven major banks including JP Morgan Chase. With the proliferation of fraud and scams has come the increased concern by U.S. lawmakers and regulators regarding consumer protection. After being faced with the option to either pursue a settlement or face an enforcement action by the Consumer Financial Protection Bureau (CFPB), JP Morgan Chase has stated that they are considering suing CFPB. A JP Morgan Chase spokesperson claimed that "the CFPB is fully aware we already go above and beyond what the law requires, reimbursing for all unauthorized transactions and even for certain types of scams." This comes after a decrease in the percentage of fraud reimbursements across JPMorgan Chase, Bank of America, and Wells Fargo from 62% in 2019 to 38% in 2023. When it comes to scams, Jamie Dimon has previously told lawmakers that it was unreasonable to require banks to refund transfers from scams in which customers were tricked into approving payments (Microsoft Start Article). This explains the large discrepancy in reimbursements for scams which, in 2023, JP Morgan Chase only reimbursed 2% of all reported scams (Daily HODL Article). These negative actions and sentiments regarding consumer protection could explain the drop in JP Morgan Chase's stock, as it does not aline with how they advertise themselves as customer-focused, anticipating customer needs, and never allowing short-term profits to get in the way of doing what is right for the customer (JP Morgan Chase's *How We Do Business* Page).

The inconsistency in messaging and actions occurs not only with the customers but also with the employees. According to TeamBlind, JP Morgan Chase has an employee rating of 3.5/5 stars. While this rating is fairly standard compared to its competitors, the majority of the complaints seem to be directed towards their compensation and benefits with only 2.9/5 stars.

INTEGRATION AND ANALYSIS

Data Integration

When aiming to find out what kind of rudimentary data was readily available regarding JP Morgan Chase's public-facing resources, it is crucial to first find out what is the bare minimum an attacker could find with minimal skills or resources. By running basic commands to discover IP addresses and passing these initial values into WHOIS and Shodan, we can discover what pieces of their tech infrastructure are visible and analyze whether or not this poses a security risk to the company.

Part of understanding how an attacker might penetrate a system is understanding why they might target a particular company's system. This is why it is also important to consider JP Morgan Chase's relationship with the public, their stock values, and whether they maintain positive relationships with their employees as well as their customers. This part of the process involves integrating data from social media, news outlets, JP Morgan Chase's public-facing website, and anonymous professional communities such as TeamBlind. This provides not only how an adversary might penetrate a system, but also why, and if the motivation for a potential attack is anticipated, may provide the security team with a more targeted method for asset prioritization and threat mitigation.

Cross-Verification

In comparison with Glassdoor, JP Morgan Chase's rating was lower by 0.5 stars on TeamBlind. However, Glassdoor did not give the same breakdown that TeamBlind did where the number of stars given for each review was an average of the ratings for the following categories: Career Growth, Compensation/Benefits, Management, Work-Life Balance, and Company Culture. While implications are made that the drop in stock price was due to their response to a push to increase consumer protections, this link has yet to be verified.

RECOMMENDATIONS

Further investigations of the experience of JP Morgan Chase's employees on anonymous dashboards would be crucial in getting a better idea of any systemic/chronic issues with the company's working environment, structure, and process to anticipate any causes for animosity. Delving deeper into what pieces of the tech infrastructure are visible/available to the public will be crucial to identifying potential attack vectors.

It would be beneficial for JP Morgan Chase to dedicate some of their public relations resources towards their social media presence. Especially, as a new generation gains information and insight into companies' policies, culture, and products from social media platforms as opposed to press releases. Use the technical details outlined here to evaluate which aspects of JP Morgan Chase's tech infrastructure are most vulnerable. Conduct vulnerability assessments and investigate the rest of the IP addresses associated with the jpmorganchase.com domain. Understanding how and why an attacker might (try) to breach a system is vital to mitigating the risk of that attacker becoming successful and damaging the company's data and reputation.

CHALLENGES AND LESSONS LEARNED

Some challenges included access to detailed employee reviews on professional forums such as TeamBlind or Glassdoor and the rudimentary nature of the technical information gathered. Doing breadth-focused investigations across multiple professional forums may provide more data points when identifying any causes for animosity from JP Morgan Chase employees. Additionally, the technical information collected was very rudimentary and may not account for attackers with more knowledge or resources.

CONCLUSION

This information-gathering initiative provided basic details on what public information about JP Morgan Chase's tech infrastructure could be used as a potential attack vector. This includes information on IP addresses, hostnames, SSL certificates, encryption methods, and domain status codes. Through searching trending news articles, it was discovered that JP Morgan Chase's attitude towards consumer protection laws might be a possible motivation for an attack. The lack of engagement on JP Morgan Chase's social media accounts does not help attract customers or build positive customer relationships. Finally, examining potential insider threats by looking at posts on anonymous professional forums also provides information on how, why, or when a likely attack may occur.