NVIDIA CORPORATION

Submitted by Group 1

1. **Pragya Mittal**
2. **Yu-An Tsai**
3. **James Volante**

Basic Profile

Name: NVIDIA Corporation
Headquarters Location: 2788 San Tomas Express Way, Santa Clara, CA 95051
Website: https://www.nvidia.com/en-us/
Ticker Symbol: NVIDIA Corp, NASDAQ: NVDA

Company Assets

1. **NVIDIA Graphic Processing Unit (GPU) Intellectual Property (Specific):** It includes the plans and schematics of their proprietary GPU.
2. **Financial Systems (General):** Unauthorized access could lead to financial and privacy losses.
3. **Employee Database (General):** Breach of employee data poses a risk for the company and opens it up to a privilege escalation attack.
4. **Manufacturing Plants for NVIDIA's chips (Specific):** NVIDIA, unauthorized access could disrupt the supply chain.
5. **R&D Data (Specific):** If stolen, other rival companies can use it to gain a strategic advantage over NVIDIA.
6. **Customer Information Database (General):** A breach could lead to lawsuits and reputational damage.
7. **ERP System (General):** Unauthorized access could disrupt business processes.
8. **Email System (General):** We need to safeguard this to protect against social engineering attempts.
9. **Cloud Infrastructure (General):** If availability is lost, the company could lose profit.
10. **Point-of-Sale Terminals (Specific):** NVIDIA has restaurants on some campuses that employees frequent.

Competitor with NVIDIA

Motives: Dominate more space within the Chip Industry. Financial.

Skills:

- Skilled teams of lawyers
- Employees tend to have an advanced understanding of malicious tools and how to deploy them.
- Teams have been made within the organization to understand software vulnerabilities, and potentially how to exploit them.

Background:
AMD (Advanced Micro Devices) is an American corporation within the chip industry. Some of their products include
GPUs, CPUs, and software. AMD focuses heavily on R&D to stay ahead of its competitors. [1]

Misuse Cases
Since AMD is within the same sector as NVIDIA, there is a lot of relatability within the work they do. The companies have collaborated before [2], meaning AMD could have a high understanding of their IT infrastructure. With vast amounts of resources, it can easily hire dark web investigators to scan the dark web for any breaches, hire the best lawyers to pursue litigation and disrupt operations within the company, and even exploit the relation that the CEO of AMD and NVIDIA have (NVIDIA CEO is uncle to CEO of AMD)

Goals and Motives
The organization is highly motivated to take more market space that NVIDIA controls. With recent news of NVIDIA's success within the AI industry [3], AMD would also like to capitalize on that same success.

Attack Scenario:
AMD can hire a recently fired/laid-off NVIDIA worker. This employer may know the IT Infrastructure and how to breach their systems. Once he would gain access, he could steal R&D data to give AMD an edge, or even try to halt operations within a company so they fall behind in the market.

Actor: Business Competitor

Threat Type: Targeted

Access Type: Insider Threat

Access Point: Employees Credentials

Attack Pattern:

1. Social Engineering
2. Data Exfiltration
3. Disruption Tactics

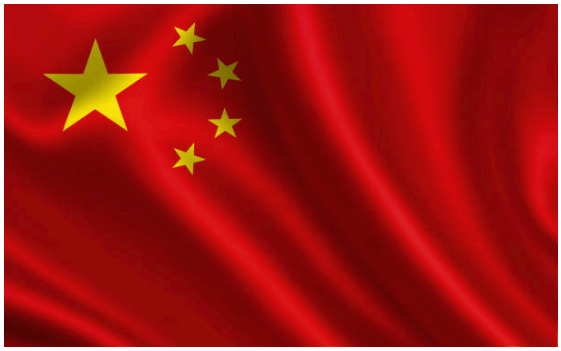
Direct Consequence:

1. Loss of competitive advantage
2. Operational Downtime
3. Reputation damage

Human Impact	**Adversary Motivation**	**Adversary Resources**	**Adversary Methods**
Job Insecurity	Gain Market Share	Former NVIDIA worker	Insider Recruitment
Stress	Money	Abundant financial resources	Social Engineering
Potential Layoffs	Disrupt operations	Tools	Data Theft

China

Nation-State Cyber Actor



Motives

Political motives: to fight for technological dominance; to disrupt the relationship between the US, China, and Taiwan

Skills [4][5][6]

- Heavily invested government-sponsored and independent cyber unit
- Known for carrying out sophisticated advanced persistent threat activities
- State-sponsored cyber group Volt Typhoon

Background

According to CISA, China remains the most active and persistent cyber threat to the US government, private-sector, and critical infrastructure networks. [7] Recent years, the US government has issued export controls of computer chips to China to impede AI breakthroughs that could benefit the Chinese government.

Misuse Cases

The Chinese government would likely have one of the state-sponsored cyber units to perform cyber attacks. According to CISA, exploiting public vulnerabilities is a common cyber attack tactic of Chinese State-sponsored cyber operations. [8] Therefore, it is likely that the cyber attack unit would utilize vulnerabilities within NVIDIA's IT infrastructure to carry out the attack.

Goals and Motives

China could be motivated by ensuring its technological dominance on AI development and military advancement. China could also be motivated by disrupting anything or anyone that poses a threat to the "One China" policy.

Attack Scenario

The Chinese government will likely delegate the task of cyber attack to a state-sponsored cyber attack organization. Then the cyber attack organization would first scan NVIDIA's Internet to find open ports to infiltrate. They would then attempt to exploit known vulnerabilities in NVIDIA's IT environment, and further deploy malware to execute the exfiltration of confidential documents.

Actor: Nation State Cyber Attacker

Threat Type: Targeted

Access Type: Network access

Access Point: Public-facing application / Network access

Attack Pattern:

1. Vulnerability Abuse
2. Social Engineering
3. Credential Stealing

Direct Consequence:

1. Confidential Data Leakage (Confidentiality)
2. Interruption of System Operation (Availability)
3. Geopolitical Shock

Human Impact	**Adversary Motivation**	**Adversary Resources**	**Adversary Methods**
Innovation Slowdown	Technological Dominance	Expertise	Data Exfiltration under Multi-phase Attack
Tension in International Relationship	Political Justice	Expertise and Money	Multi-phase Attack

Ricky Thompson

Former Data Center Engineer

Age: 35
Sex: Male
Education: Master of Science in Computer Science
Motives: Financial gain and personal revenge

Skills

Experience with NVIDIA's data center, including knowledge on NVIDIA's own product and network infrastructure

Background

Ricky Thompson is a former employee of NVIDIA. He quit his job because of poor work-life balance around 2022, just before the global AI craze. He is envious of the company's recent success and stock price.

Misuse Case

Ricky Thompson has knowledge on the operation of NVIDIA's data center and infrastructure. He could use the knowledge to identify vulnerabilities within the data center to either exfiltrate confidential data or crash the data center. He could also sell confidential data to interested personnel.

Goals and Motives

Ricky Thompson would be motivated to extract confidential data from NVIDIA and sell it to NVIDIA's competitors, stockholders, or other government. He would also be motivated to crash NVIDIA's IT environment and systems to retaliate on NVIDIA for his loss.

Attack Scenario

Ricky Thompson is familiar with the infrastructure of NVIDIA's IT environment, so it is likely that he exploits the vulnerability in the network and systems, gains access and escalated privileges into the environment, and either directly exfiltrate data or crash systems by deploying malware or modifying configurations.

Actor: Disgruntled Former Employee

Threat Type: Targeted

Access Type: Network Access

Access Point: Network Access

Attack Pattern: Vulnerability Abuse

Direct Consequence:

1. Confidential Data Leakage (Confidentiality)
2. Interruption of System Operation / Gaming Service (Availability)
3. Destruction or Deletion of Data (Integrity)

Human Impact	**Adversary Motivation**	**Adversary Resources**	**Adversary Methods**
Loss of Client Trust	Financial Gain	Expertise	Data Exfiltration
Delayed Product Release	Personal Revenge	Inside Knowledge	Denial of Service under Multi-phase Attack
Increased Employee Workload	Social Justice	Expertise and Time	Configuration Modification through Multi-phase Attack

Preyrana Mishra

Senior Director of Product Management

Age: 39
Sex: Female
Education: MBA from Tepper, Bachelor's in Computer Science Engineering
Motives: Financial gain and personal revenge

Skills
Familiarity with product lifecycle and products in the process of being launched. Understanding of the financial, product, and operational data. Knowledge of common cybersecurity practices and circumvention tactics

Background
Preyrana Mishra is the Senior Director of Product Management at NVIDIA. She recently got passed over by a more underqualified male counterpart for the role of Chief Product Officer.

Misuse Cases
Preyrana has extensive insight into the internal workings of the product lifecycle, processes, and policies of the company. She also has access to NVIDIA's financial data. She has privileged access to the internal communication.

Goals and Motives
Preyrana's primary goal is to expose NVIDIA's unfair promotion policies by leaking internal documents and communiques related to executive decision-making. She could also be motivated by revenge and may want to cause financial harm by leaking product information before it hits the market.

Attack Scenario
Preyrana could plan to exfiltrate confidential data like internal financial reports. She could access these internal reports by gaining unauthorized access to the CEO's office. She could do this by social engineering or by compromising the Access Card mechanism either by cloning Jansen's card using an RFID cloner or scrambling the scanner altogether.

Actor: Disgruntled Current Employee

Threat Type: Insider Threat

Access Type: Privileged access to sensitive corporate data

Access Point: Corporate emails, cloud storage

Attack Pattern: Data Exfiltration
Corporate Sabotage
Covert Operations

Direct Consequence: Reputation Damage (confidentiality)
Financial Impact (availability)
Legal Repercussions (availability)

Human Impact	**Adversary Motivation**	**Adversary Resources**	**Adversary Methods**
Resentment	Exposing	Insider Knowledge	Social Engineering
Empowerment	Revenge	Privilege access	Data Exfiltration
Financial Wellbeing	Money	Technical expertise	Multi-phase attack

BitJustice League

Hacktivist Group

Education: Varied, members may be anywhere from high school graduates to certified Master's or PhD candidates
Motives: Social Justice / Political Activism

Skills

1. Proficiency with anonymity tools and techniques
2. Advanced hacking and programming skills
3. Research, Investigative and reverse engineering skills
4. Proclivity to engage in anarchy and civil disobedience

Background

BitJustice League was founded by a group of highly skilled and passionate individuals (betraying their nerdy side with the nod to Batman in their name) who have been frustrated by the bureaucratic red tape and want to take social change into their own hands. They target corporations that don't align with their ideals on environmentalism, human rights, and accountability. Members come from various backgrounds, including IT, law, and social sciences, bringing a diverse set of skills and perspectives.

Misuse Cases

This group is highly motivated and skilled at finding vulnerabilities within systems like NVIDIA's. They could use their technical and social engineering skills to gain remote access to internal servers, escalate their privilege, and move laterally within the system all while masking their presence in the system.

Goals and Motives

The main goal of BitJustice League is to keep companies honest and accountable and raise awareness about the internal practices of NVIDIA and whether they are sustainable and socially responsible. They aim to speak truth to power and believe in full transparency, whatever the means to gain that information and whatever impact of that information being made public may be.

Attack Scenario

BitJustice League could initiate a multi-phase attack by sending out convincing phishing emails to gain unauthorized access to internal systems and deploying ransomware encrypting critical infrastructure and services until some corrective action is taken by NVIDIA or financial compensation is given to BitJustice League.

Actor: Hacktivist Organization

Threat Type: Ideologically motivated

Access Type: Remote access through software vulnerabilities

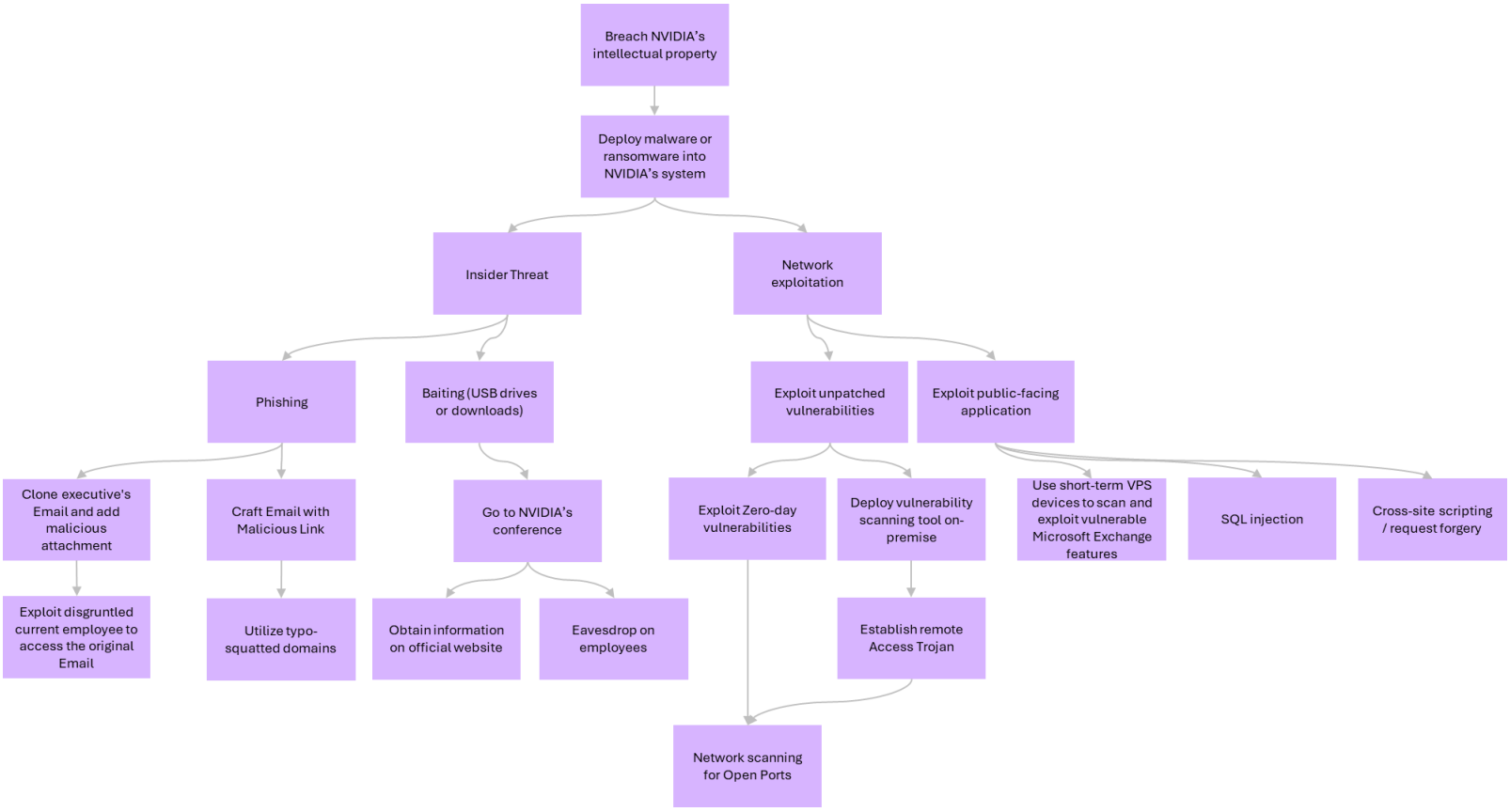
Access Point: Corporate web applications, internal systems

Attack Pattern: Exploiting known vulnerabilities in widely used software
Data exposure and leak
Denial of service (DoS)

Direct Consequence: Overwhelm web servers (availability)
Leak sensitive information (confidentiality)
Manipulate financial reports (integrity)

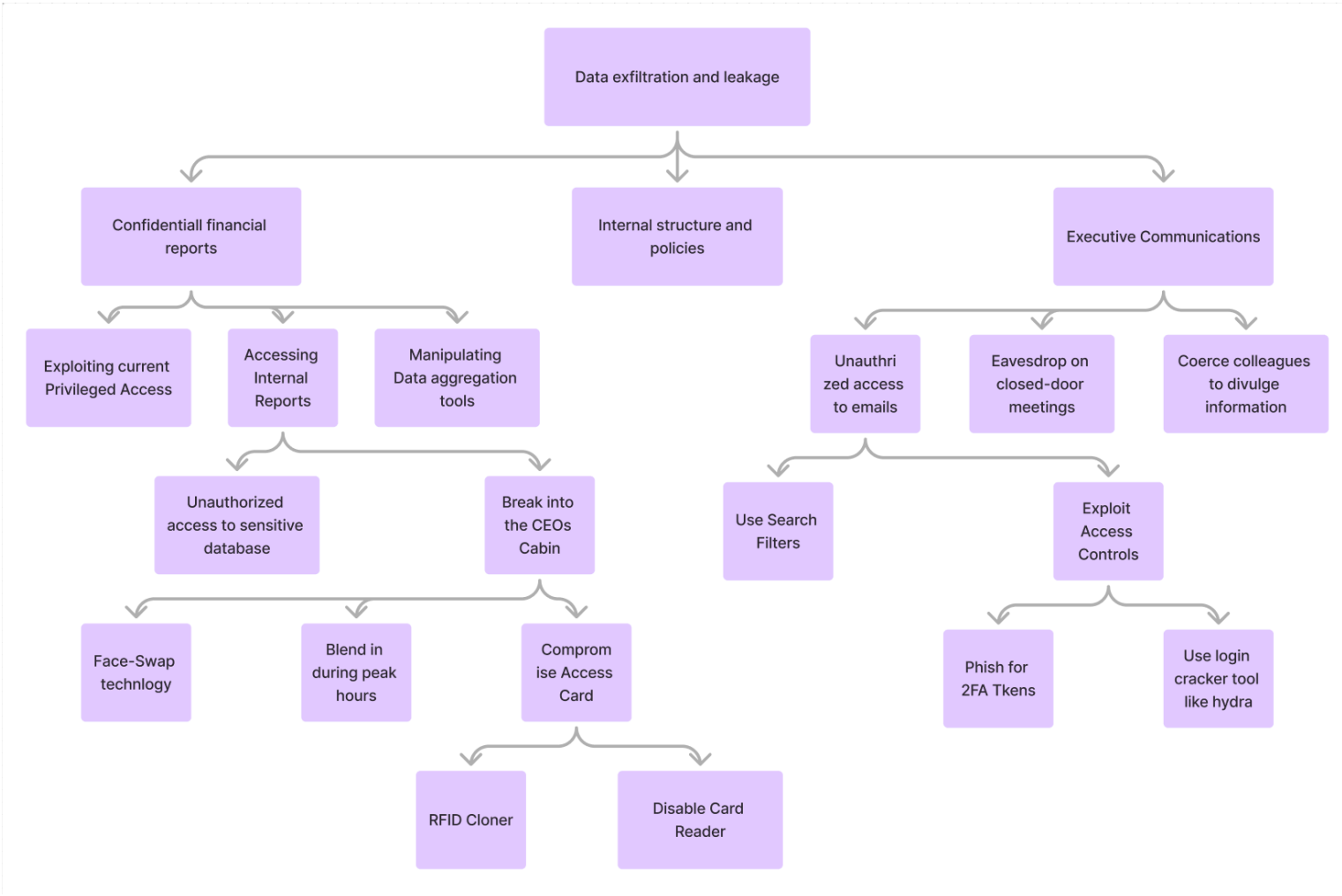
Human Impact	**Adversary Motivation**	**Adversary Resources**	**Adversary Methods**
Fulfillment of Principles	Social Justice	Hacker community support	Web Application Exploits
Bragging rights	Chaos and disruption	Penetration tools	Data Exfiltration
Financial Wellbeing	Accountability within corporations	Technical expertise	Data Poisoning

Attack Tree for China



Reference: Common TTPs of Chinese State-Sponsored Cyber Operations [9]

Attack Tree for Preyrana Mishra



Letter to Jensen Huang

Dear Jensen Huang,

It has recently come to our attention that some of the data we found within the reconnaissance intel package had very detailed personal information about you. In order to lessen the damage and prevent future leaks of your personal info, we have devised some guidance that will assure your personal life will be kept hidden and secure. A high profile individual such as you needs to be secure at all times, as you are one of the biggest targets within NVIDIA.

The first step that we would recommend you do is to make sure none of your passwords are vulnerable. Within the intel package, we found some of your prior old passwords, and it is of the utmost importance that you update all of your passwords, and make sure none are vulnerable. Generally speaking, a good cybersecurity practice to have is to have a password manager manage your passwords. If you don't have one already, I would highly recommend getting one in order to make sure your passwords are more secure.

Another way to protect yourself from social engineering attacks is to remain vigilant about the people that contact you. If someone contacts you impersonating a vendor or from the company, always verify their identity in any way. A lot of social engineering attacks try to build a foundation of trust with you in order to gain access within the company, but someone as high profile as yourself will be targeted consistently, so always make sure the person you are talking to is the person they actually claim to be.

One of the most successful social engineering attacks are phishing attacks. The same advice here applies, always remain vigilant against emails that may be suspicious. Before clicking on any URL within an email, hover over it and see where the URL would actually send you. If the URL is malicious, then you may notice the URL looks a little weird, and if that's the case, report the email. Another good way to notice phishing attempts is to look at the email senders and domain name. Malicious addresses may tend to look like it came within the company, but they usually have a misspelling in it. That is a dead giveaway for a phishing attempt.

If you follow this guidance, this would help you be aware of any potential attacks that may be focused on you. Thank you for reading this letter.

Letter to Camir Ricketts

Dear Camir Ricketts,

Recently, we have discovered that a lot of your own personal information has become leaked in a reconnaissance intel package. In order to help mitigate any potential damage that may be caused by this dangerous leak of your info, we are going to give you some guidance on how to avoid future cyber attack.

One of the main concerns that we found is that you had a lot of your social media profiles public. Although this may seem to be something that isn't a huge deal, attackers can actually use this information pertaining to you. We have details of your hobbies, marital status, favorite places to visit, and more just because of your publicly facing accounts. We would recommend turning them to private in the future.

We also found you had some vulnerable passwords that were posted on the dark web. These passwords are very critical to the safety of your personal accounts, such as your financial accounts, personal social media accounts, and any other websites you may have accounts to. It is a good practice to implement a password manager to hold and generate random passwords.

Phishing attacks are also some of the most common ways people end up getting hacked. Phishing refers to the process of scammers trying to steal your personal information, while impersonating someone of trust. The number one way they gain access to systems using phishing is using email phishing. They send an email asking for sensitive information, from what seems to be a reputable source. However, this is usually not the case. To protect yourself against these attacks, always look at the senders email address, never put personal information on an email and send it, and if you're gut tells you its a scam, it probably is.

Although these may seem small and a waste of time, they will greatly enhance your personal security and make you more resistant to social engineering. Your privacy is something we value here at NVIDIA, and we hope that you take these steps in order to protect yourself, and other of your close friends from potential harm. We thank you for your cooperation.