islington college

(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Risk, Crisis & Security Management

Assessment Weightage & Type

50% Individual Coursework

Year and Semester

2023-24 Autumn

Student Name: David Budha Magar

London Met ID: 22068721

College ID: np01nt4a220119

Coursework Due Date: 05, Jan 2024

Coursework Submission Date: 02, Jan 2024

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Table of Contents

Table of Figure

1. Introduction

Cybersecurity is the process of protecting networks, devices, and data against unauthorised access and illegal use, while also ensuring the confidentiality, accuracy, and accessibility of information. Cybersecurity is also known as information security (Agency, 2021).

Vulnerabilities include technical flaws, human error, and outside threats. Risk assessment lists potential dangers and ranks them by severity risk management mitigates, shifts, or embraces them. Information security, business continuity, regulatory compliance, and public perception are all risk management "security measures" in this context. Reliable cyber security systems must improve to combat cyber threats to ensure data availability, integrity, and confidentiality.

1.1. Aim

The main aim of this project is to study Nvidia's cyberattack and offer a thorough analysis of Risk Management and Risk Control as they pertain to such incidents.

1.2. Objectives

- Conduct an inquiry into the event. Investigate Nvidia's hacking problem using credible sources.
- Perform a comprehensive analysis of the attack. Analyse the techniques employed by the **LAPSUS$** organisation to infiltrate Nvidia's systems.
- Consider past events' significance. Examine the cyber attack's history and other threats.
- Analyse the response Evaluate Nvidia's risk mitigation tactics in addressing the assault.

2. Background

2.1. Risk Management

Risk
Management
['risk 'ma-nij-mənt]
The process of identification, analysis, and acceptance or mitigation of uncertainty in investment decisions.
Investopedia

Figure 1:Risk Management Source: (Kenton, 2023)

Risk management is the systematic approach of recognising, assessing, and managing potential risks to an organization's financial, legal, strategic, and security aspects that could impact its capital and revenues. The potential risks or perils could result from various origins, including economic instability, legal accountability, errors in strategic management, accidents, or catastrophic occurrences. The Risk Management process consists of three crucial steps (IBM, 2023):

1. **Identifying Risk:** Risk identification refers to the systematic process of identifying and analysing potential threats and hazards that may pose risks to a firm, its operations, and its personnel. Identifying hazards such as malware, ransomware, accidents,

natural catastrophes, and other potential disruptions to corporate operations is a part of assessing IT security threats (IBM, 2023).

2. **Risk Analysis and Assessment:** Risk analysis is evaluating the probability of a risk event transpiring and the probable outcome of each instance. The level of each hazard is assessed and categorised based on its prominence and impact. (IBM, 2023).
3. **Risk Mitigation and Monitoring:** Risk mitigation is the act of creating and conducting plans and methods to reduce the impact of potential risks on project goals. A project team may employ risk mitigation strategies to identify, monitor, and evaluate the potential risks and consequences associated with the successful completion of a certain project, such as the development of a new product. Risk mitigation refers to the actions made to address concerns and manage the implications of difficulties that may arise in a project (IBM, 2023).

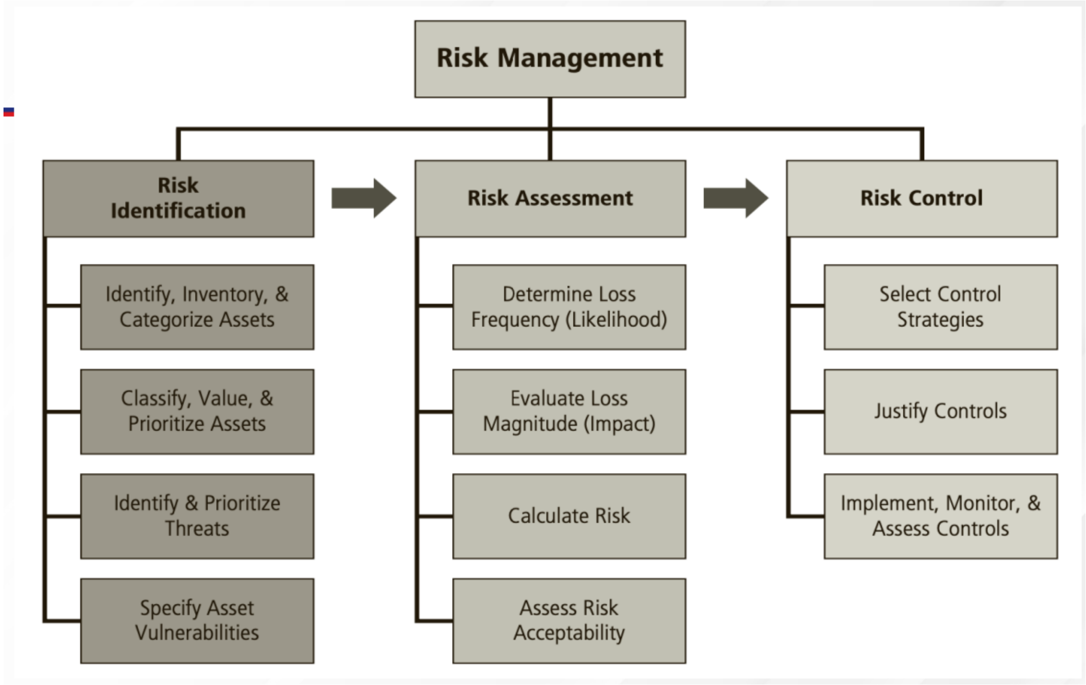

Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Determine Loss Frequency (Likelihood)
Evaluate Loss Magnitude (Impact)
Calculate Risk
Assess Risk Acceptability
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

Figure 2:Risk Management Process Source: Week 3 Lecture PDF

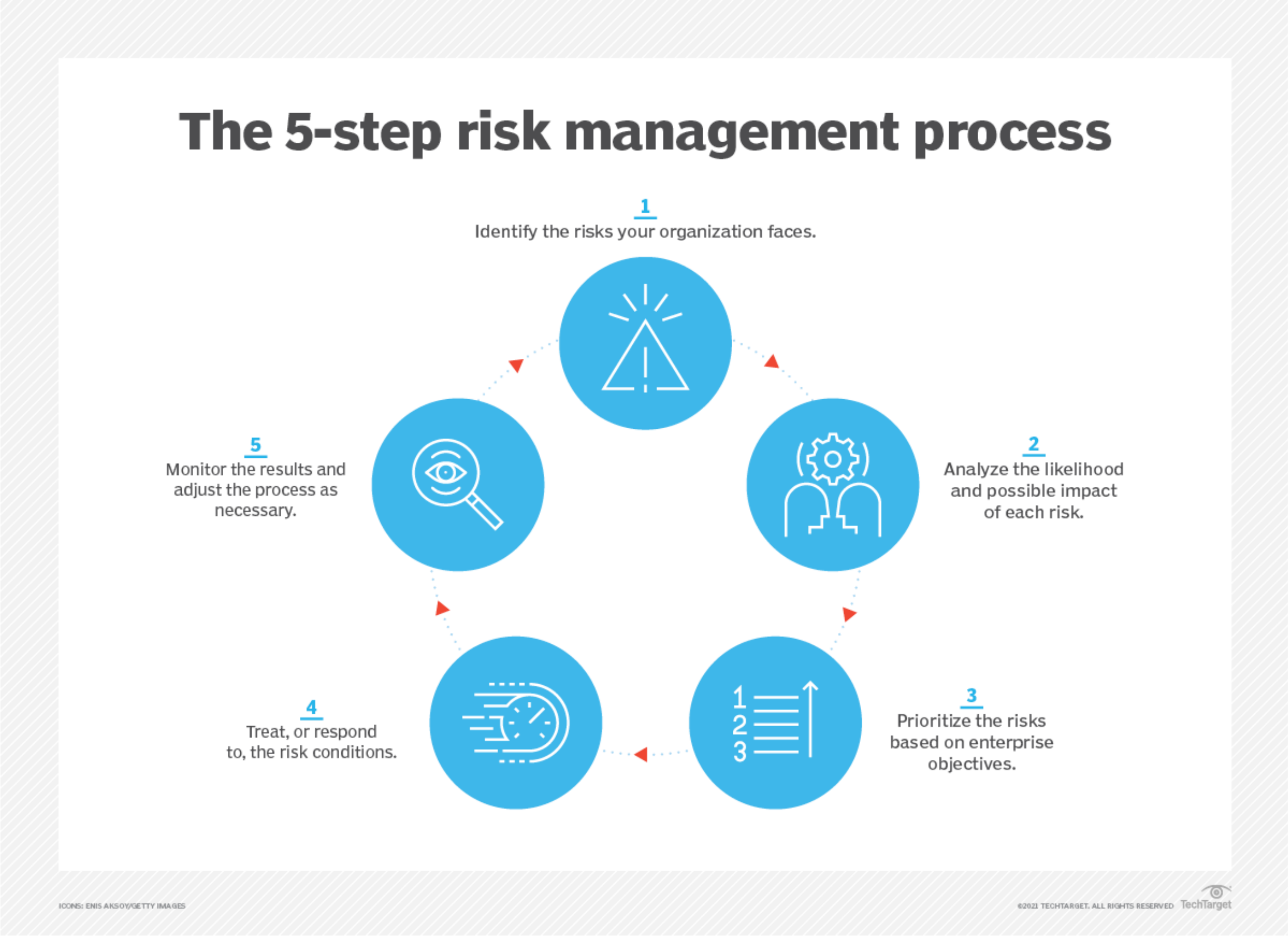

The 5-step risk management process
1
Identify the risks your organization faces.
2
Analyze the likelihood and possible impact of each risk.
3
Prioritize the risks based on enterprise objectives.
4
Treat, or respond to, the risk conditions.
5
Monitor the results and adjust the process as necessary.
ICONS: ENIS AKSOY/GETTY IMAGES
©2021 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Figure 3: Steps of Risk Management Process Source: (Tucci, 2023)

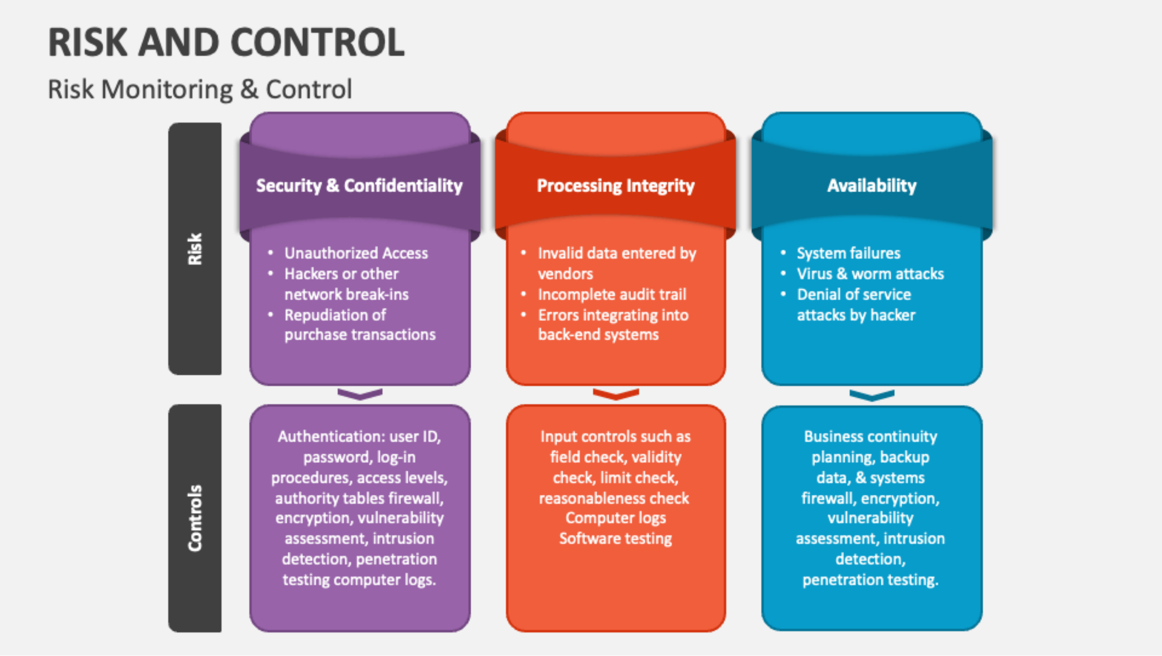
2.2. Risk Control

Risk Control
['risk kən-'trōl]
The set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats.
Investopedia

Figure 4: Risk Control Source: (Bhasin, 2023)

Risk control refers to the set of techniques employed by firms to evaluate potential losses and implement measures to mitigate or eliminate these risks. This approach utilises the findings of risk assessments, which entail identifying potential risk factors in an organization's operations, encompassing financial policies, non-technical and technical business aspects, and other elements that could influence the company's performance (Kenton, 2023).

Some of the risks that may impact the Confidentiality, Integrity, and Availability of an organization and its control measures are stated in the figure given below:



RISK AND CONTROL

Risk Monitoring & Control

Risk

Controls

Security & Confidentiality

- Unauthorized Access
- Hackers or other network break-ins
- Repudiation of purchase transactions

Authentication: user ID, password, log-in procedures, access levels, authority tables firewall, encryption, vulnerability assessment, intrusion detection, penetration testing computer logs.

Processing Integrity

- Invalid data entered by vendors
- Incomplete audit trail
- Errors integrating into back-end systems

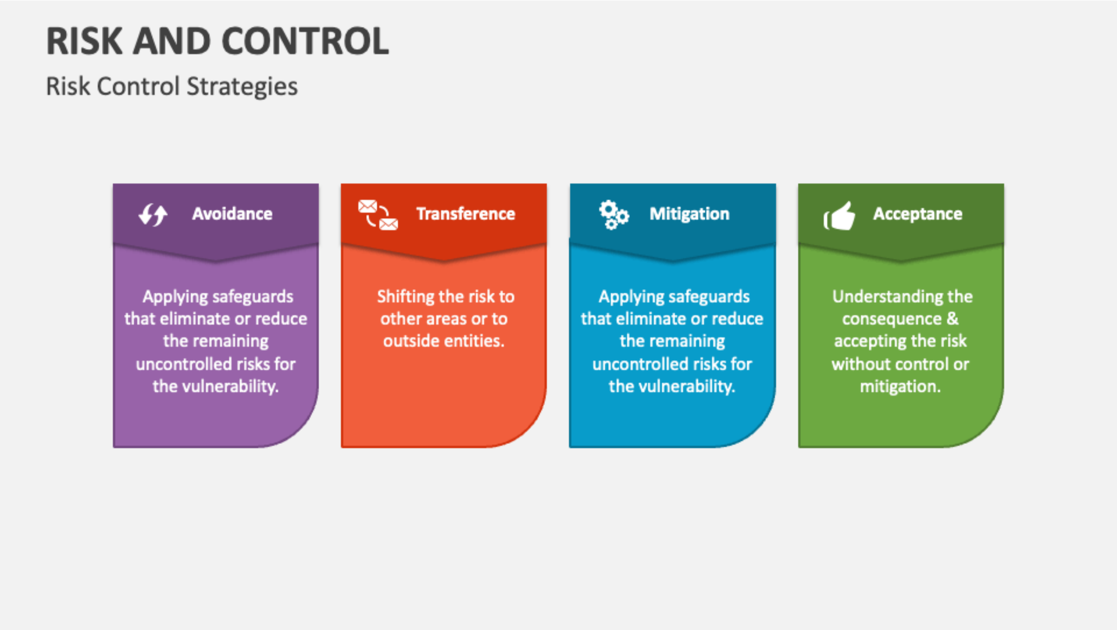
Input controls such as field check, validity check, limit check, reasonableness check Computer logs Software testing

Availability

- System failures
- Virus & worm attacks
- Denial of service attacks by hacker

Business continuity planning, backup data, & systems firewall, encryption, vulnerability assessment, intrusion detection, penetration testing.

Figure 5:Risk and Control source: (Collidu, 2023)



RISK AND CONTROL

Risk Control Strategies

Avoidance

Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability.

Transference

Shifting the risk to other areas or to outside entities.

Mitigation

Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability.

Acceptance

Understanding the consequence & accepting the risk without control or mitigation.

Figure 6: Risk Control strategies Source: (Collidu, 2023).

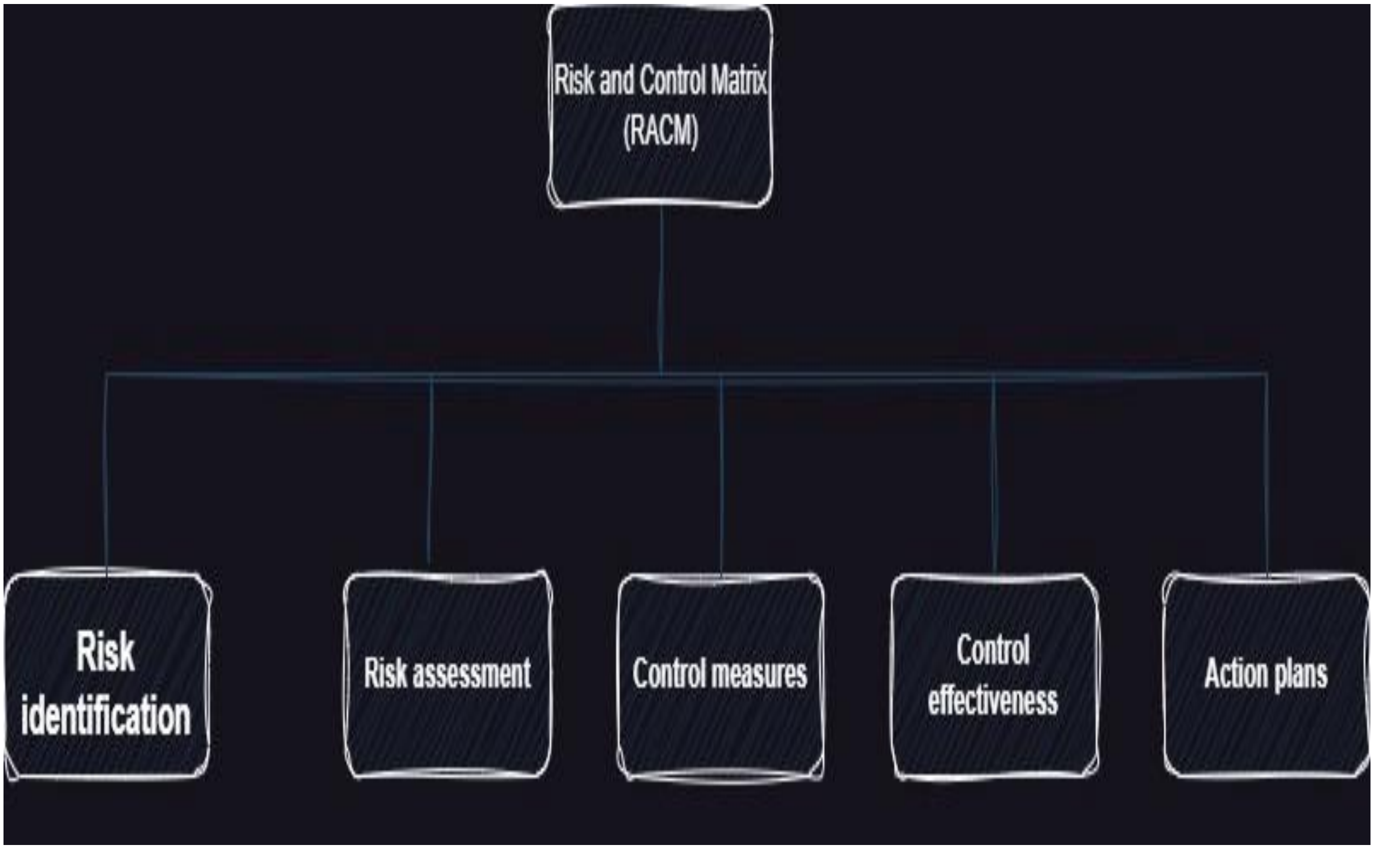


Figure 7:Risk and Control Matrix Source: Myself.

3. Literature Review

This is the case study of **Nvidia a graphic chip manufacture company** which was attacked by **Lapsus$** and lost **1 terabyte** of data on February 23, 2022.

3.1. **Case Study**: **NVIDIA**

Figure 8: Nvidia Logo Source: (Nvidia, 2023)

NVIDIA, established in 1993 under the leadership of CEO **Jensen Huang**, is a trailblazer in the field of accelerated computing. The introduction of the GPU in 1999 revolutionized the field of PC gaming, altered the realm of computer graphics, and ignited the period of contemporary artificial intelligence. NVIDIA, with a workforce of over 27,000 individuals, achieved a revenue of $18 billion in the third quarter of fiscal year 2024. Additionally, they are presented with a market opportunity worth **$1 trillion**, and are actively transforming many industries with their data-centre-scale products. It possesses over 7,500 patents, helps 4.5 million developers, and helps 16,000 entrepreneurs worldwide. Jensen Huang has been acknowledged as a "Best Place to Work in 2023" on Glassdoor and has been acclaimed as the "World's Best Performing CEO" by Harvard Business Review (Nvidia, 2023).

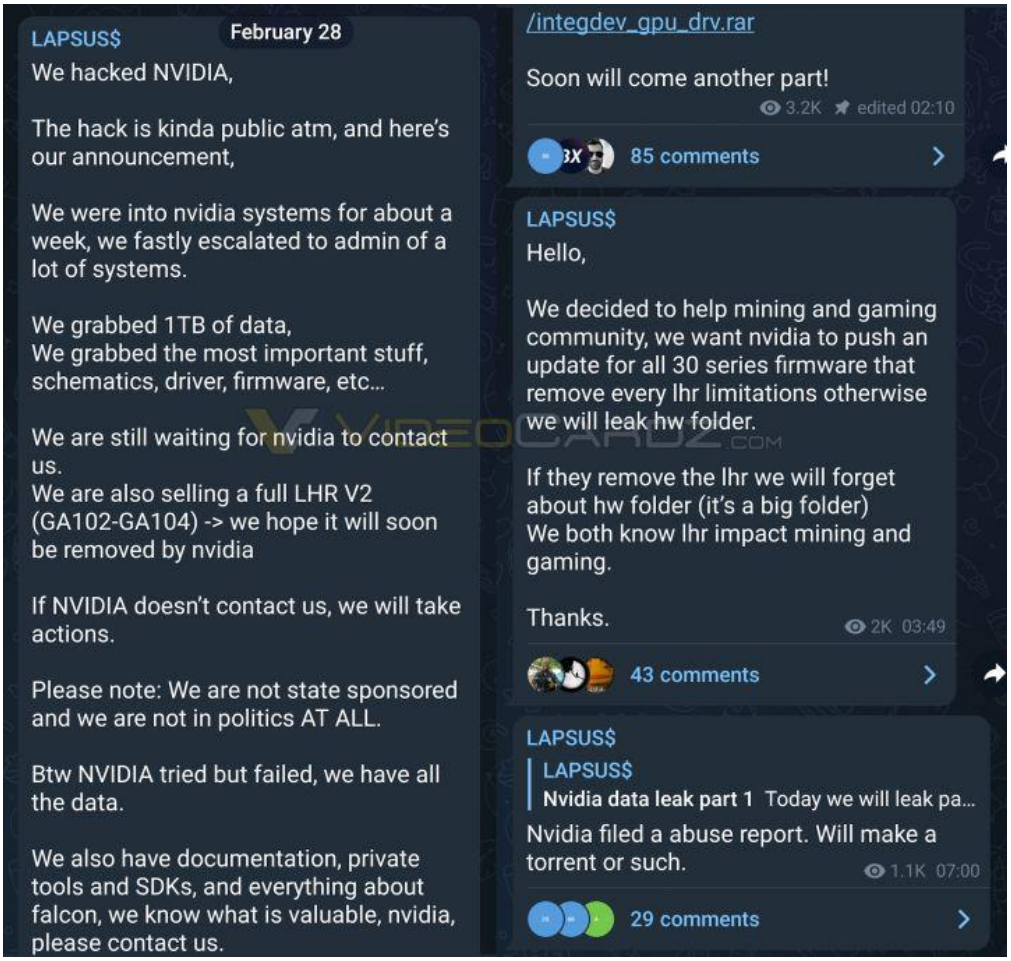
The **LAPSUS$** group, otherwise identified as **DEV-0357** by **Microsoft**, is an unstructured coalition of malicious actors lacking distinct political associations. Although regarded as amateurish even within the realm of ransomware gangs, they have effectively focused on and coerced significant amounts of money from prominent technology businesses. The gang, presumed to have originated from South America and having members worldwide, conducts its activities openly through the platforms of Telegram and email. In March 2022, the Metropolitan Police of London apprehended seven individuals associated with **LAPSUS$**, although only two of them were formally accused. The arrests, based on intelligence provided by a group targeted by **LAPSUS$**, had minimal effect on the group's activities, since they persist in exploiting and publicly disclosing the data of their victims. The **LAPSUS$** organization is distinguished by their noncompliance with commitments, transparent communication, and a disruptive attitude to cyber activities (BlackBerry, 2023).

3.1.1. Finding:

Lapsus$ launched an attack on Nvidia on February 23, 2022. Consequently, the credentials of employees and the password hashes of Windows accounts were compromised. Lapsus$ requested an unspecified sum of money, the disclosure of GPU driver source code, and the elimination of Nvidia graphics card restrictions for cryptocurrency mining. Nvidia may have complied, but sensitive data was subsequently disclosed. Nvidia issued a public statement recommending customers to update their passwords, enlisted the services of a cybersecurity company, and bolstered their security measures. The intrusion into the internal systems might have resulted in operational disruptions and raised worries about productivity. The experience emphasised the significance of proactive safeguarding for all companies amidst the increasing prevalence of ransomware threats (Trevor, 2022).

LAPSUS$ hacked Nvidia's server for **a week**. **Schematics**, **drivers**, **firmware**, and more were given in **1 terabyte**. **Falcon microprocessors** are intended for **NVIDIA GPUs**. The solution comprised **SDKs**, specialist tools, and extensive documentation (Islam, 2022) knows "LAPSUS$" value.

LAPSUS$ bypasses Nvidia GPU LHR V2 for GA102-GA104 devices. Bypass optimises RTX 30-series GPU mining. After selling the bypass, Nvidia may have contemplated buying it. LAPSUS$ reportedly forced Nvidia to remove LHR ("lite hash rate") limits from its 30 series GPU firmware. The group threatened to reveal vital secrets to get Nvidia's cooperation. The group also encouraged Nvidia to act if cooperation fails (Islam, 2022).



LAPSUS$

February 28

We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.

/integdev_gpu_drv.rar

Soon will come another part!

3.2K edited 02:10

85 comments

LAPSUS$

Hello,

We decided to help mining and gaming community, we want nvidia to push an update for all 30 series firmware that remove every lhr limitations otherwise we will leak hw folder.

If they remove the lhr we will forget about hw folder (it's a big folder)
We both know lhr impact mining and gaming.

Thanks.

2K 03:49

43 comments

LAPSUS$

LAPSUS$

Nvidia data leak part 1 Today we will leak pa...

Nvidia filed a abuse report. Will make a torrent or such.

1.1K 07:00

29 comments

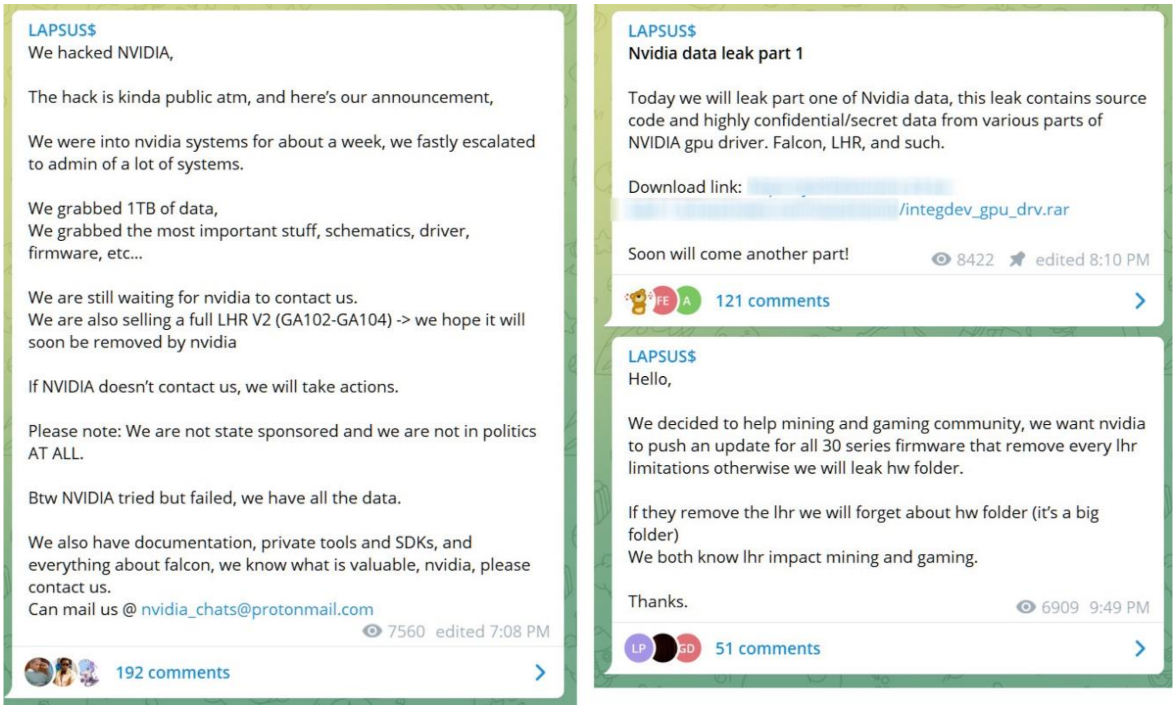
*Figure 9: LAPUS$ claims on **NVIDIA** stolen data Source: (Islam, 2022)*

Nvidia launched an assault on LAPSUS$. The occurrence encompassed the utilisation of device encryption, a demand for ransom, and subsequent retaliatory hacking. The counterattack achieved partial success as LAPSUS$ managed to secure a backup. The hackers infiltrated Nvidia's networks by exploiting Mobile Device Management and VPN. The defensive manoeuvre executed by Nvidia was recognised and appreciated due to its significant scale and significance. The corporation admitted the problem, lodged a fraud complaint, and guaranteed the uninterrupted flow of commercial transactions. Bloomberg stated that the computer breach was of minimal significance and not connected to geopolitical matters. Despite the event, Nvidia's stock price had a 1.7% increase, following an 18% decline in 2022 *(Islam, 2022)*.

Malicious GPU drivers were created by LAPSUS$ using illegal security certificates. System drivers were compromised with malware, according to the report. Antivirus scans miss this software since it uses Nvidia's credentials. The corrupted certificates infected computers without alarms, posing a major threat. The user reported the following attack identifier (Murray, 2022):

- **43BB437D609866286DD839E1D00309F5**
- **14781bc862e8dc503a559346f5dcc518**

This information applies to manually downloaded Nvidia drivers. Using Nvidia Experience to automatically download drivers is secure (Murray, 2022).



LAPSUS$
We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.
Can mail us @ nvidia_chats@protonmail.com

LAPSUS$
Nvidia data leak part 1

Today we will leak part one of Nvidia data, this leak contains source code and highly confidential/secret data from various parts of NVIDIA gpu driver. Falcon, LHR, and such.

Download link: [redacted]/integdev_gpu_drv.rar

Soon will come another part!

LAPSUS$
Hello,

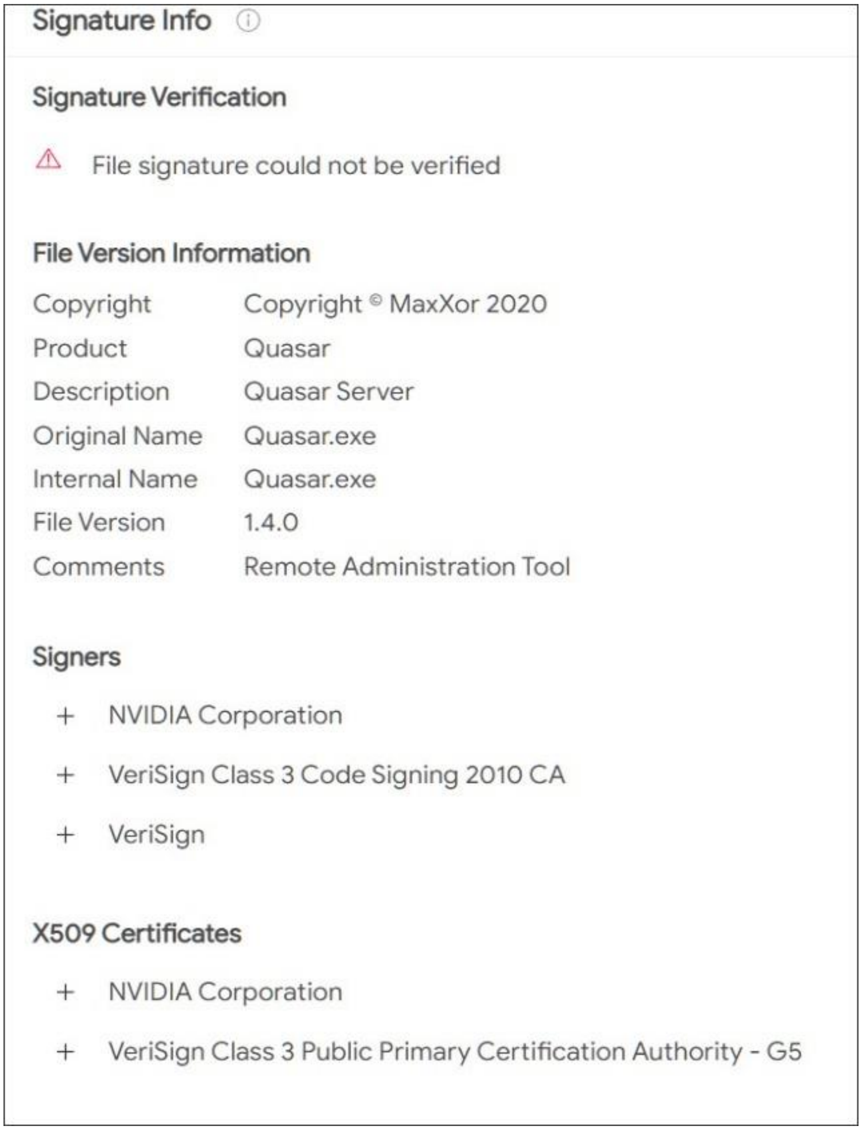
We decided to help mining and gaming community, we want nvidia to push an update for all 30 series firmware that remove every lhr limitations otherwise we will leak hw folder.

If they remove the lhr we will forget about hw folder (it's a big folder)
We both know lhr impact mining and gaming.

Thanks.

*Figure 10: **Lapsus$** messages about **NVIDIA** Attack Source: (Abrams, 2022)*

The perpetrators were malicious. A cyberattack used NVIDIA code-signing certificates to endorse malicious software. Windows loads expired driver certificates. Malicious programmes might imitate legitimate ones, posing security issues. Microsoft recommends Windows Defender Application Control rules for NVIDIA driver management. However, non-technical users may have installation issues. Microsoft's revocation of stolen certificates may improve security but prevent the usage of authorised NVIDIA drivers. According to VirusTotal malware scanning samples, the stolen certificates were used to digitally sign harmful software and hacking tools. These included **Mimikatz, backdoors, Cobalt Strike beacons**, and **remote access trojans**. One attacker signed a **Quasar** remote access trojan **[VirusTotal]** with the certificate, while another certified it. User mentioned Windows driver *(Abrams, 2022)*.



Signature Info ⓘ

Signature Verification

⚠ File signature could not be verified

File Version Information

Copyright	Copyright © MaxXor 2020
Product	Quasar
Description	Quasar Server
Original Name	Quasar.exe
Internal Name	Quasar.exe
File Version	1.4.0
Comments	Remote Administration Tool

Signers

+ NVIDIA Corporation

+ VeriSign Class 3 Code Signing 2010 CA

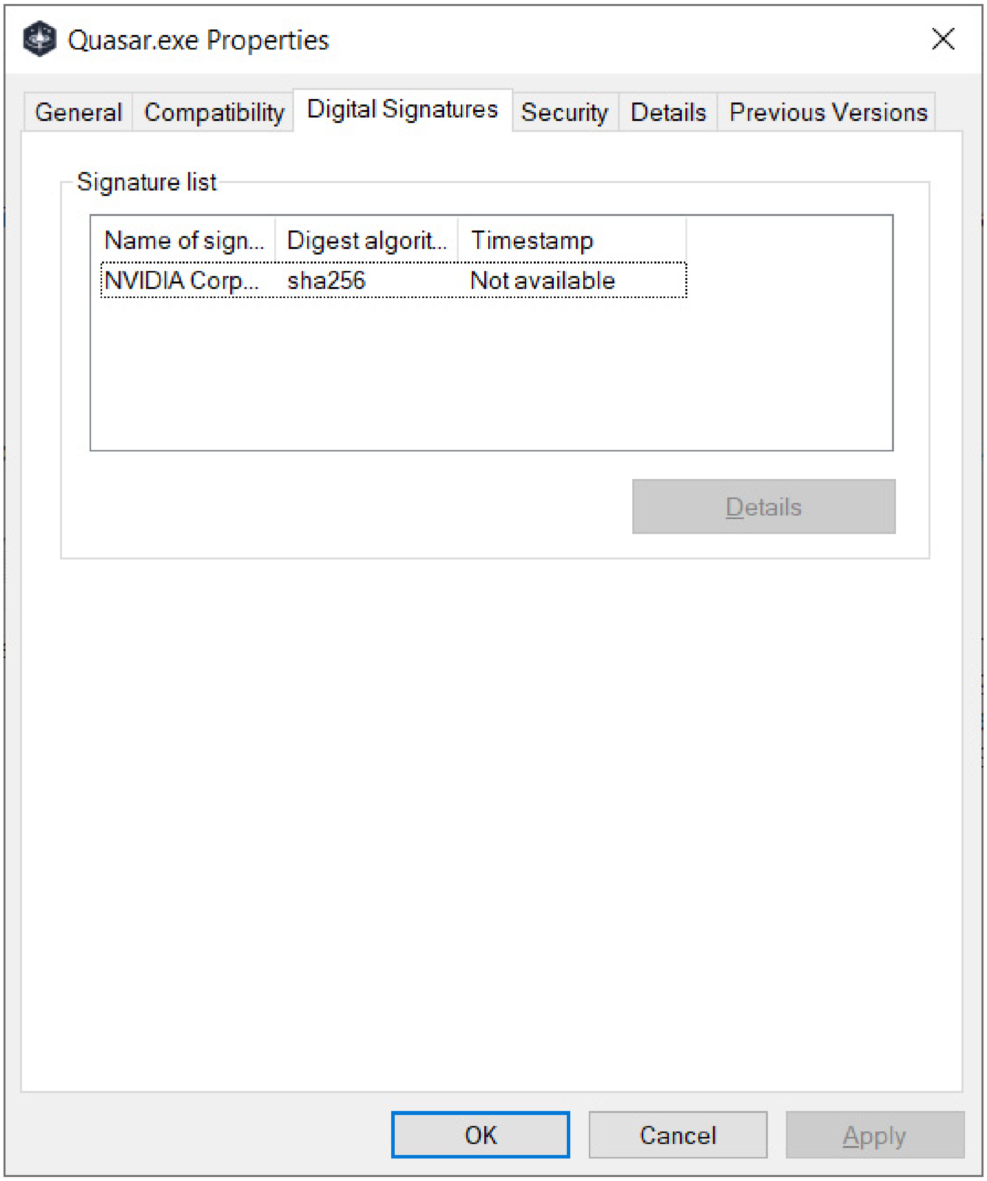
+ VeriSign

X509 Certificates

+ NVIDIA Corporation

+ VeriSign Class 3 Public Primary Certification Authority - G5

Figure 11:Quasar RAT signed by NIVIDA certificate Source: (Abrams, 2022)



Name of sign...	Digest algorit...	Timestamp
NVIDIA Corp...	sha256	Not available

Figure 12: Signed Quasar RAT sample Source: (Abrams, 2022)

3.1.2. Analysis:

The data breach serves as a stark warning about the need for robust security procedures, which must be implemented and thoroughly tested to avoid future tragedies like the one that occurred to the Nvidia company.

Preventive Measures:

1. **Enhanced Network Security:**
   - **Risk Identification:** Consistently evaluate and pinpoint vulnerabilities in the network infrastructure, such as deficiencies in Mobile Device Management and VPN systems.
   - **Risk Mitigation:** Enforce robust network security protocols, such as firewalls, intrusion detection systems, and routine security audits.
2. **Multi-Factor Authentication (MFA):**
   - **Risk Identification:** Acknowledge the potential dangers linked to compromised employee credentials.
   - **Risk Mitigation:** Implement multi-factor authentication to enhance security by introducing an extra level of protection, hence increasing the difficulty for unauthorised individuals to get access.
3. **Regular Security Audits and Penetration Testing:**
   - **Risk Analysis:** Examine the efficacy of current security measures.
   - **Risk Mitigation:** Perform routine security audits and penetration testing to actively detect and resolve weaknesses in systems and applications.
4. **Encryption of Sensitive Data:**
   - **Risk Analysis:** Evaluate the possible consequences of data breaches on the protection of sensitive information.

- **Risk Control:** Deploy encryption protocols to safeguard sensitive data, ensuring its security in the event of unauthorised intrusion.

5. **Employee Training and Awareness:**
   - **Risk Identification:** Address the potential dangers posed by social engineering assaults and human error.
   - **Risk Control:** Conduct cybersecurity education to staff members, with a focus on the significance of complying with security protocols and identifying phishing attacks.
6. **Continuous Monitoring and Threat Detection:**
   - **Risk Mitigation:** Deploy modern threat detection systems to enable ongoing monitoring of network activity.
   - **Risk Control:** Identify irregularities and possible security violations in real-time, enabling prompt action against developing cyber risks.
7. **Incident Response Planning:**
   - **Risk Mitigation:** Create and often evaluate an incident response strategy.
   - **Risk Control:** Facilitate a synchronised and efficient reaction to cyber breaches, including tactics for communication and preparations for data restoration.

Post-Incident Response:

1. **Isolation and Containment:**
   - **Risk Mitigation:** Take immediate action to isolate affected systems and prevent the further dissemination of the attack.
   - **Risk Control:** Mitigate more harm by unplugging impacted systems from the network.
2. **Engage Cybersecurity Experts:**
   - **Risk Mitigation:** Collaborate in cooperation with cybersecurity specialists and institutions.

- **Risk Control:** Engage external experts to examine the assault, identify weaknesses, and execute corrective actions.

3. **Communication and Transparency:**
   - **Risk Mitigation:** Create a comprehensive communication strategy to effectively engage with stakeholders.
   - **Risk Control:** Establish clear and open lines of communication with customers, staff, and the public in order to maintain trust and effectively handle the company's image.
4. **Data Recovery and Restoration:**
   - **Risk Mitigation:** Incorporate a comprehensive strategy for data recovery and restoration inside the incident response plan.
   - **Risk Control:** Establish and execute backup and recovery protocols to minimise both the loss of data and the duration of system outage.
5. **Legal and Regulatory Compliance:**
   - **Risk Mitigation:** Observe all applicable laws and regulations.
   - **Risk Control:** Engage in collaboration with law enforcement authorities and adhere to reporting duties in order to minimise legal repercussions.
6. **Continuous Improvement:**
   - **Risk Mitigation:** Consistently evaluate and revise risk management techniques.
   - **Risk Control:** Learn lessons from the occurrence, adapt security protocols, and strengthen the ability to withstand comparable future cyber threats.
7. **Engagement with Law Enforcement:**
   - **Risk Mitigation:** Engage in cooperation with law enforcement authorities.
   - **Risk Control:** Provide essential details to assist in the inquiry and any legal action against the assailants.

Nvidia might reduce the likelihood of assaults by executing frequent audits, utilising **multi-factor authentication**, and **establishing strong network security protocols**. Quick action, including separating compromised systems, consulting with cybersecurity experts, and maintaining open lines of communication, can mitigate the impact of an attack. Improving and adapting a cybersecurity plan on a regular basis is essential for keeping up with new threats.

4. Conclusion

In conclusion, the **Nvidia** cyber-attack highlights the significant need for effective cybersecurity **Risk Management and Risk Control** procedures. This incident highlights how important it is to be proactive with security measures, have a plan for dealing with malware, secure the supply chain, communicate openly before, during, and after an attack, **update firmware and software** often, think about the **geopolitical** and **financial consequences**, **utilise strong password management**, and **monitor constantly.** The case study's findings stress the need of responding to evolving cyber threats with a comprehensive and adaptable cybersecurity plan.

5. Bibliography

Abrams, L., 2022. *Bleepingcomputer.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/
[Accessed 17 12 2023].

Agency, C. &. I. S., 2021. *cia.gov.* [Online]
Available at: https://www.cisa.gov/news-events/news/what-cybersecurity
[Accessed 22 11 2023].

Anon., n.d. [Online].

Bhasin, H., 2023. *MARKETING91.* [Online]
Available at: https://www.marketing91.com/what-is-risk-control/

BlackBerry, 2023. *BlackBerry.* [Online]
Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lapsus
[Accessed 27 12 2023].

Chen, K. Y., 2021. *A Systematic Approach for Cybersecurity Risk Management,* s.l.: Kristin YiJie Chen.

Collidu, 2023. *Collidu.* [Online]
Available at: https://www.collidu.com/presentation-risk-and-control
[Accessed 14 12 2023].

Collidu, 2023. *Collidu.* [Online]
Available at: https://www.collidu.com/presentation-risk-and-control
[Accessed 14 12 2023].

Consulting, M., 2020. *mha-it.com.* [Online]
Available at: https://www.mha-it.com/2020/01/29/risk-management/
[Accessed 04 12 2023].

IBM, 2023. *ibm.com.* [Online]
Available at: https://www.ibm.com/topics/risk-management
[Accessed 11 12 2023].

institute, G. r. m., 20232. *grm.institute.* [Online]
Available at: https://grm.institute/blog/why-do-we-study-risk-management/
[Accessed 04 12 2023].

Islam, Z., 2022. *digitaltrends.* [Online]
Available at: https://www.digitaltrends.com/computing/hackers-stole-top-secret-gpu-details-then-nvidia-hit-back/
[Accessed 16 12 2023].

Kenton, W., 2023. *Investopedia.* [Online]
Available at: https://www.investopedia.com/terms/r/risk-control.asp#:~:text=Risk%20control%20is%20a%20plan-based%20business%20strategy%20that,may%20interfere%20with%20an%20organization%27s%20operations%20and%20objectives.
[Accessed 11 12 2023].

Kenton, W., 2023. *Investopedia.* [Online]
Available at: https://www.investopedia.com/terms/r/riskmanagement.asp
[Accessed 01 01 2024].

Kenton, W., 2023. *investopedisa.com.* [Online]
Available at: https://www.investopedia.com/terms/r/risk-control.asp

Murray, S., 2022. *THEGAMER.* [Online]
Available at: https://www.thegamer.com/hackers-fake-gpu-drivers-nvidia/
[Accessed 16 12 2023].

Nvidia, 2023. *Nvidia.* [Online]
Available at: https://media.iprsoftware.com/219/files/202311/corporate-nvidia-in-brief-pdf-december-3056300-r2-2.pdf?Signature=%2FkU8Bue%2FXGWEm8izFqZ9gZL7%2BWk%3D&Expires=1703690568&AWSAccessKeyId=AKIAJX7XEOOELCYGIVDQ&versionId=Kg1wCZP.LuqFtUOJi3dAakvjMU.DGF27&respons
[Accessed 27 12 2023].

Trevor, A., 2022. *vpnreactor.* [Online]
Available at: https://www.vpnreactor.com/nvidia-cyber-attack/
[Accessed 13 12 2023].

Tucci, L., 2023. *Techtarget.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important
[Accessed 01 01 2024].

Valeros, V., 2019. *Stratosphere Lab.* [Online]
Available at: https://www.stratosphereips.org/blog/2019/2/17/what-do-we-know-about-quasar-rat-a-review
[Accessed 21 12 2023].

6. Appendix

One of the most important and fastest growing areas of technology is cybersecurity. According to a study conducted by Cybersecurity Ventures, cybersecurity experts predict that by 2021, cybercrime will cost the global economy $6.1 trillion annually. Driven by the pandemic, cybercrime is expected to soon become the world's third largest economy. Cyber security Ventures predicts that global cybercrime costs will increase by 4,444 percent annually over the next five years, from $3 trillion in 2015 to $10.5 trillion annually by 2025. That is why banks, technology companies, healthcare, government agencies, and every other industry are investing in cybersecurity infrastructure to protect the 4.444 billion customers who trust them with their business and personal information. It is not surprising that it is. This section describes historical examples of cybersecurity incidents. The creation and evolution of major cybersecurity frameworks and standards are reviewed to provide a deeper understanding of existing cybersecurity approaches (Chen, 2021).

Understanding and identifying cybersecurity risks is critical to personal protection Key terms are:

1. Hacker, attacker, or intruder: An individual who exploits weaknesses in software for personal gain. Purposes range from harmless curiosity to malicious activities such as stealing or altering information (Agency, 2021).
2. Malicious Code (Malware): Unwanted files or programs that damage or compromise data. Examples: Viruses, worms, and Trojan horses. Characteristics include requesting user action, distribution without intervention, and deceptive behaviour (Agency, 2021).
3. Vulnerability: A flaw in software, firmware, or hardware that can be exploited by an attacker. Programming error results in illegal action being possible (Agency, 2021).

To minimize the risk of cyberattacks, we can follow these best practices:

1. **Keep your software up to date**: Patches that address known vulnerabilities Install. Enable automatic operating system updates (Agency, 2021).
2. **Run your current antivirus software**: Detect, isolate, and remove several types of malwares. Enable automatic virus definition updates for maximum protection.
3. **Use a strong password**: Choose a password that is difficult to guess. Use a long and secure passphrase of at least 16 characters.
4. **Change the default username and password**: Malicious attackers can easily access default credentials. Change default settings to strong and unique passwords.
5. **Implementing multi-factor authentication (MFA)**: Verify user identity using at least two of her components. Minimizes the risk of unauthorized access even if your password is compromised.
6. **Install a firewall**: Prevents some attack vectors by blocking malicious traffic. Limit unnecessary outbound communications. Enable and configure the firewall according to device or system specifications.
7. **Be suspicious of unexpected emails (phishing):** Phishing emails are intended to obtain information, steal money, or install malware. Beware of unexpected emails.

By adopting these cybersecurity best practices, individuals can increase their personal protection against a variety of cyber threats.

Risk = (threat x vulnerability (exploit likelihood x exploit impact) x asset value) - security controls

There are four main approaches to managing hazards in the intricate field of IT risk management and they are:

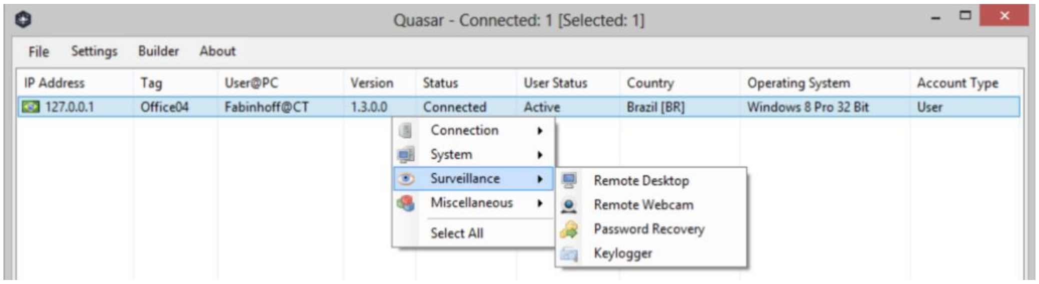
1. **Risk avoidance**: Applying steps to remove or decrease the vulnerability's remaining uncontrolled risks.
2. **Risk transference**: transferring the risk to different regions or external parties.
3. **Mitigation:** Minimizing the damage if the vulnerability is used.
4. **Risk Acceptance**: Recognizing the effects and accepting the risk in the absence of mitigation or control.

6.1. Risk and Control Matrix (RACM)

Organizations can utilize a Risk and Control Matrix (RACM) to better analyse and improve their risk profiles. The RACM includes the following components (Kenton, 2023):

- **Risk identification:** The matrix reviews all potential hazards that an organization may encounter, and is frequently organized by business sectors, processes, or activities (Kenton, 2023).
- **Risk assessment:** Each risk is evaluated based on its chance of occurrence and impact on the company. This evaluation assists in prioritizing risks and directing resources to the most crucial regions (Kenton, 2023).
- **Control measures:** The matrix highlights the exact control measures applied for each risk to mitigate or lessen the chance and impact of the risk. These measures may include policies, processes, systems, or other risk-management techniques (Kenton, 2023).
- **Control effectiveness:** The RACM assesses the efficacy of each control measure, taking into consideration aspects such as compliance, control design adequacy, and the control's capacity to identify or prevent the risk from materializing (Kenton, 2023).
- **Action plans:** The matrix may contain action plans for enhancing risk control measures or correcting identified gaps in the organization's risk management processes based on the assessment of control effectiveness (Kenton, 2023).

6.2. What is Quasar RAT?



IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
127.0.0.1	Office04	Fabinhoff@CT	1.3.0.0	Connected	Active	Brazil [BR]	Windows 8 Pro 32 Bit	User

Figure 13: Quasar RAT UI showing a list of infected victims, and some of the capabilities of the RAT. Source: (Valeros, 2019)

According to **MaxXor's GitHub** repository, Quasar is a Remote Access Tool/Trojan that was developed in July 2014. The RAT was once referred to as **xRAT**. The creator rebranded the software as Quasar RAT after its initial release as version 1.0.0.0 in August 2015. Quasar, a remote administration tool (**RAT**) written in C#, is compatible with the following operating systems: Windows XP SP3, Windows Server 2003/2008/2012, Windows 7, 8/8.1, and 10. The **MIT** License allows for unrestricted distribution, modification, personal use, and commercialization of the code. Since its inception, there have been more than 900 forks and extensive evolution (Valeros, 2019).

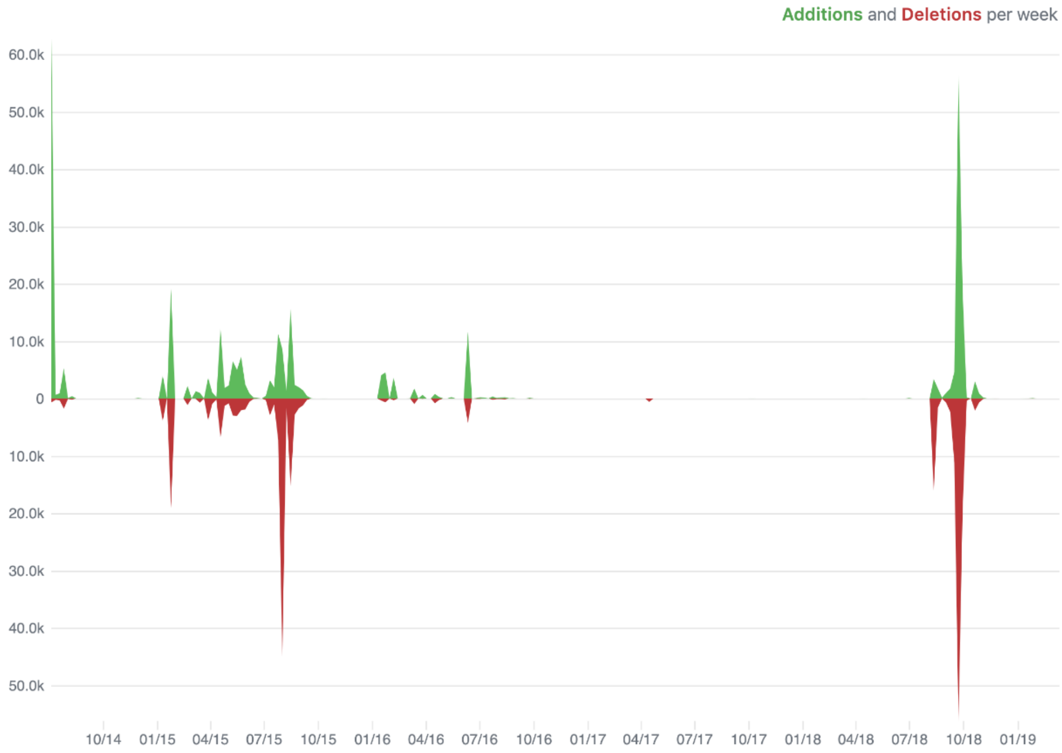


Figure 14: Code Frequency Quasar RAT since its origin in 2014. Source: (Valeros, 2019)

Thanks to its reliability and intuitive design, **Quasar** is touted by the author as a multipurpose tool for user assistance, administrative duties, and staff monitoring. The project intends to incorporate more secure and user-friendly features into the tool, and its capabilities are being enhanced (Valeros, 2019).

- **Task Manager**
- **File Manager**
- **Startup Manager**
- **Remote Desktop**
- **Remote Shell**
- **Download & Execute**
- **Upload & Execute**

- **System Information**
- **Computer Commands (Restart, Shutdown, Standby)**
- **Keylogger (Unicode Support)**
- **Password Recovery/Stealing (Common Browsers and FTP Clients)**
- **Registry Editor**

Quasar is beneficial for performing routine administrative duties daily. Potential adversaries seldom disregard an open-source project of this nature. Palo Alto Networks' analysis in January 2017 revealed that the Gaza Cybergang organization employed the Downeks downloader during their September 2016 **'DuskSky'** attack to distribute the Quasar RAT. Downeks and Quasar were featured in an article by **TripWire** in February 2017 (Valeros, 2019).

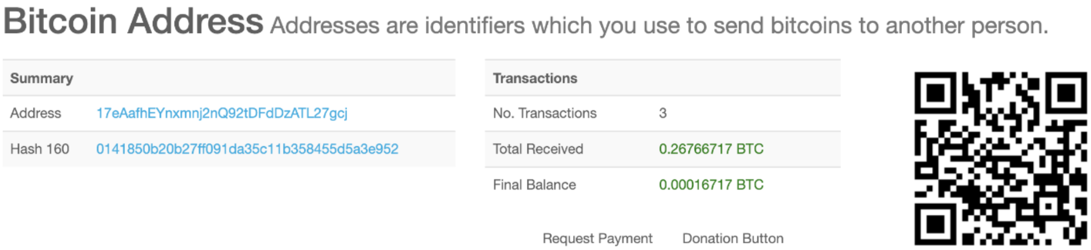
In April 2017, PwC published research about the most recent actions of APT10. Since 2016, researchers have seen that the threat actor has enhanced their tools, such as Quasar RAT, by using open-source technologies. According to the study, ATP10 has been using Quasar RAT since early 2017 (Valeros, 2019).

TrendMicro found Patchwork or Dropping Elephant as an espionage group in December 2017. The gang employed Quasar RAT in many operations against government and diplomatic entities in 2017. Operate a motor vehicle-The RAT was provided through downloads (Valeros, 2019).

In January 2018, Palo Alto Networks Unit 42 disclosed that Quasar RAT and **VERMIN** were employed in deliberate assaults against Ukraine starting from late 2015. In July of the same year, ESET provided a comprehensive account of the ongoing deliberate attacks on Ukraine government agencies with the purpose of espionage and data theft.

According to ESET, **Quasar RAT** was employed in conjunction with **Vermin** and **Sobaken**. **Quasar** is not the first nor final open-source remote access trojan. **AsyncRAT, Powershell-RAT, Lime-Controller**, **microRAT**, and **pupy RAT** are just a few examples of the many remote access trojans (**RATs**) that may be downloaded for free.

Certain variants of Quasar RAT exhibit intriguing characteristics. One of the options allows for donations in BTC to be made to the wallet with the address: **17eAafhEYnxmnj2nQ92tDFdDzATL27gcj**. Despite its apparent lack of activity, the fork has received several donations, as evidenced by the image below (Valeros, 2019).



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	17eAafhEYnxmnj2nQ92tDFdDzATL27gcj
Hash 160	0141850b20b27ff091da35c11b358455d5a3e952

Transactions	
No. Transactions	3
Total Received	0.26766717 BTC
Final Balance	0.00016717 BTC

Figure 15:A fork [23] from Quasar RAT is accepting donations to help the project move forward. Source: (Valeros, 2019)