CARDING

Executive Summary -

This report provides an in-depth analysis of carding attacks, a prevalent form of cybercrime involving the unauthorized use of stolen credit card information. It explores the methods and techniques employed by cybercriminals, delves into the wide-ranging impact and consequences of such attacks, and outlines preventive and mitigation strategies. Through case studies of significant incidents like the Target Data Breach and the Equifax Data Breach, the report offers real-world insights. Additionally, it discusses current trends, such as increased sophistication and automation, and provides a future outlook that considers emerging technologies and regulatory changes. In conclusion, this report underscores the critical importance of understanding, preventing, and responding to carding attacks in the ever-evolving cybersecurity landscape.

1.Introduction about Carding -

Carding refers to the unauthorized use of credit cards to obtain goods or services fraudulently. It is a criminal activity and is a significant issue in the world of online transactions. Carders use various methods to steal personal financial data from unsuspecting victims, which can then be used for illicit purposes, such as purchasing products online without the consent of the cardholder or selling the data to other criminals.

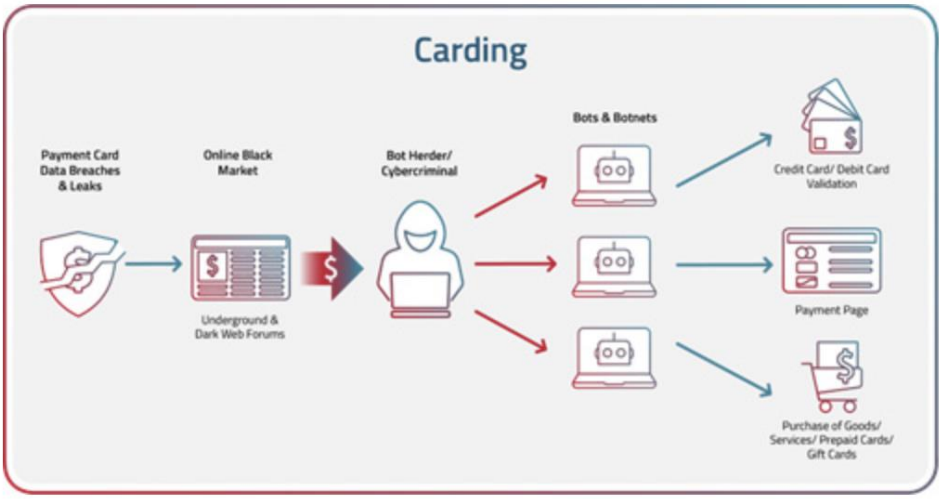
According to the Federal Trade Commission (FTC), consumers lost $627 million to fraud in the last few years. And online shopping was the third most reported type of fraud.

2.Definition of Carding -

Carding is the process of fraudulently obtaining and using credit or debit card information to purchase goods, services, or to conduct financial transactions without the knowledge or consent of the cardholder.

3.Methods and Techniques of Carding -

- Phishing: Criminals use fake emails, websites, or messages to trick individuals into providing their card details. These emails often look like they come from legitimate sources but are designed to steal information.
- Skimming: A small device, known as a skimmer, is placed on card-reading devices such as ATMs or gas pumps. When a person uses their card, the skimmer captures the card's information.
- Data Breaches: Cybercriminals can break into companies' databases to steal a vast amount of user data, including credit card details. These can later be sold on the dark web.
- Malware and Spyware: These are malicious software programs that can be installed on a person's computer without their knowledge. They can record keystrokes or capture data, which can then be sent to criminals.
- Physical Theft: This is the direct theft of a person's credit or debit card.
- Carding Forums: Online forums where carders buy, sell, and exchange information and stolen data.
- RAM Scraping: This technique involves malware that infiltrates point-of-sale (POS) systems to extract card data from the system's RAM where it is briefly stored in an unencrypted format during transaction processes.



4.Impact and Consequences of Carding:

Carding, also known as credit card fraud, has significant negative impacts and consequences:

- Financial Loss: Cardholders and financial institutions suffer financial losses due to unauthorized transactions.
- Reputation Damage: Businesses and individuals affected by carding may experience damage to their reputation, making it harder to trust them.
- Legal Consequences: Perpetrators can face criminal charges, leading to fines and imprisonment.
- Regulatory Compliance: Businesses may be subject to fines and legal action if they fail to implement adequate security measures.
- Consumer Confidence: Carding incidents erode consumer confidence in online and offline payment systems.

5.Prevention and Mitigation Strategies:

To prevent and mitigate carding, various strategies can be employed:

- Secure Payment Systems: Implement robust encryption and secure payment gateways.
- Two-Factor Authentication (2FA): Require 2FA for transactions and account access.
- Regular Monitoring: Continuously monitor transactions for suspicious activity.
- Educate Employees: Train employees to recognize phishing attempts and follow security protocols.
- Regular Software Updates: Keep software and systems up to date to patch vulnerabilities.
- Risk Assessment: Conduct regular risk assessments to identify potential weaknesses.

- Fraud Detection Tools: Employ advanced fraud detection tools and algorithms.

The Top 5 Most Common Carding Attacks:-

1. Phishing by impersonating a bank representative
2. Buying your details on carding forums
3. Tricking your into installing malware
4. Using credit card skimming or shimming devices
5. Hacking a website's payment system

6.Case study -

- Home Depot Data Breach (2014): Home Depot experienced a massive data breach where cybercriminals compromised the point-of-sale systems in their stores. This attack resulted in the theft of credit card information from approximately 56 million customers. Like the Target breach, it had severe financial and reputational consequences for the company. The attackers were linked to a group of Eastern European hackers.

- Magecart Attacks: Magecart is a group of cybercriminals known for injecting malicious code into e-commerce websites' payment forms. They have successfully stolen credit card data from various online retailers by compromising the checkout process. These attacks have targeted well-known companies, including British Airways, Ticketmaster, and Newegg, among others.

7a. Websites that had been attacked by the carders?

- Home Depot website this was also being used by the carders for the attack.
- Equifax website which was being used by the carders.

7b. Software or tools that are being used in carding -

- Skimmers is a tool for debit/credit machine for which they fix camera for finding pin number and card details.

- DarkApp - This software is not like the dark web, but only the designs I created myself and the tools I created. I got the idea to design the darkapp from movie hacker 2016. +++{ Update Version 0.3 }+++ - Feature Tracking CCTV - Added Feature Tracking IP Address - Added Upload Picture Profile - Added Feature Virtual Carding - Added Feature Free Proxy

8.Current Trends in Carding:

- Sophisticated Techniques: Carding methods have become more sophisticated, with cybercriminals using advanced tools and tactics to bypass security measures.
- Darknet Marketplaces: Carding products and services are often bought and sold on underground marketplaces on the dark web, making it harder for law enforcement to track down perpetrators.
- Automation: Automation tools, known as "carding bots," are increasingly used to carry out large-scale carding operations, making it easier to target multiple victims simultaneously.
- Stolen Data Trade: The sale of stolen credit card data continues to thrive on the dark web, providing a steady supply of information for carders.
- Phishing and Social Engineering: Cybercriminals use phishing emails and social engineering techniques to trick individuals into revealing their credit card information.

9.Future Outlook for Carding:

- AI and Machine Learning: Both carders and security professionals are expected to leverage AI and machine learning to enhance their techniques and countermeasures.
- Biometric Authentication: As biometric authentication becomes more widespread, carders may shift their focus to finding ways to compromise these systems.
- Regulatory Changes: Governments and regulatory bodies are likely to enact stricter regulations and penalties to deter carding and protect consumers.

- Increased Collaboration: Businesses, law enforcement agencies, and cybersecurity firms may collaborate more closely to share threat intelligence and combat carding.
- Emerging Payment Technologies: As new payment technologies emerge, carders may adapt to exploit vulnerabilities in these systems.

10.Conclusion:

Carding remains a persistent and evolving threat in the world of cybersecurity. As technology advances, carders continue to adapt their tactics, making it essential for individuals, businesses, and law enforcement agencies to stay vigilant and up to date on the latest security measures. The future of carding will involve a constant arms race between cybercriminals and those working to protect against fraudulent activities.

It is important to remember that engaging in or supporting carding is illegal and unethical. Always act within the boundaries of the law and promote ethical behavior in the digital realm. If you suspect any fraudulent activity, report it to the appropriate authorities or your financial institution for investigation.

11.References -

https://answerthepublic.com/reports/e5f3a417-a6b3-4a55-baa5-97df0eea0eb8?recently_searched=true

https://www.radware.com/cyberpedia/bot-management/carding/

How do ATM skimmers work? Experts show how devices steal your credit and debit card info

https://www.stax.com/insights/the-growing-importance-of-digital-forensic-tools-in-investigating-criminal-activities

https://sourceforge.net/directory/?q=carding+software

https://ascarding.com/tags/carding-software/