Report Prepared By: Prasad Nikam

Carding

❖ Table of Contents:

1. Executive Summary:

This in-depth report delves into the dark world of carding, an illegal activity that preys on unauthorised utilisation of credit card information for personal financial gain. We investigate a variety of carding methods and techniques, shedding light on their intricate workings. Furthermore, we thoroughly investigate the far-reaching consequences of carding, which affect both individuals and businesses. To fortify organizations' defence against this nefarious practise, we present a strategic arsenal of mitigation strategies that they can use to protect their assets and reputations.

2. Introduction:

i. **Cyberattack Range:**
- Organizations as well as individuals face various cyberattacks.
- Attacks include DoS, ransomware, and data theft.

ii. **Carding Attack Blend:**
- Carding attacks combine traits of these attacks.
- Goal: Gain usable credit card data.
- Result: Verified payment card info.

iii. **Data Source Variety:**
- Cybercriminals acquire card numbers through diverse methods.

iv. **Carding Benefits:**
- Carding provides complete, validated payment details.
- Resource-heavy, affecting legitimate merchants' sites.

v. **Dual Protection Aim:**
- Combat carding safeguards:
- Prevent misuse of stolen card data.
- Reduce drain on merchants' computational resources.

vi. **Vital Self-Protection:**
- Personal safeguard from credit card theft is crucial.

vii. **Emergence of Carding:**
- Carding attacks have gained prominence in the realm of cyber threats.
- These attacks exploit vulnerabilities to access sensitive payment card data.

viii. **Hybrid Nature of Carding:**
- Carding attacks exhibit a unique blend of offensive tactics.
- They involve both data theft and resource consumption, making them multifaceted.

ix. Credit Card Data Acquisition:

- Cybercriminals acquire credit card details through various channels.
- This data forms the foundation for carding attacks.

x. Precision of Carding:

- Carding aims for accuracy and validation of stolen card information.
- Attackers strive to maximize the value of the stolen data.

xi. Resource Implications:

- Carding activities consume substantial computational resources.
- Legitimate merchants' websites often bear the brunt of these resource-intensive attacks.

xii. Economic and Security Impact:

- Carding attacks lead to financial losses for victims.
- They also undermine the security and trust of online payment systems.

xiii. Defensive Objectives:

- Defending against carding attacks serves a dual purpose:
- Preventing misuse of stolen card data by cybercriminals.
- Preserving the efficiency of legitimate merchants' platforms.

xiv. Collective Responsibility:

- Protecting against carding requires collaboration among individuals, organizations, and cybersecurity experts.
- Effective defence demands a comprehensive approach to deter cybercriminals.

xv. Risk Mitigation Strategy:

- As the threat of carding persists, organizations implement proactive measures.
- These measures curb the success rate of carding attacks while reinforcing cybersecurity.

xvi. Ethical and Legal Imperatives:

- Addressing carding involves upholding ethical standards and complying with legal norms.
- Responsible use of technology ensures the security and integrity of online transactions.

3. Definition of Carding:

- Carding is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards or purchase gift cards. Carding typically involves the holder of the stolen card or card information purchasing store-branded gift cards, which can then be sold to others or used to purchase other goods that can be sold for cash. Credit card thieves who are involved in this type of fraud are called “carders.”

- Carding, in the context of cybersecurity, refers to the illicit practice of using stolen or fraudulently acquired credit card information for unauthorized financial transactions, often for financial gain. Cybercriminals engaging in carding typically exploit vulnerabilities in online payment systems, e-commerce platforms, or databases to obtain sensitive payment card details. These details may include credit card numbers, expiration dates, cardholder names, and sometimes even CVV (Card Verification Value) codes.

- Carding attacks involve various techniques to monetize stolen credit card data, such as making unauthorized purchases, transferring funds, or selling the acquired card information on the black market. Carding can have significant financial and reputational consequences for both individuals and businesses, leading to financial losses, compromised personal information, and damaged trust in online payment systems.

4. Methods and Techniques:

➢ General methods

1. **Credit Card Scams:**
    - Fraudsters trick individuals into sharing their card details.
    - Common methods include phishing emails, SMS scams, and fake websites.
    - Victims unknowingly provide their card information to attackers.
2. **Data Breaches:**
    - Cybercriminals target organizations to steal large sets of card data.
    - Weak security measures or vulnerabilities in systems are exploited.
    - Stolen data is then sold or used for fraudulent activities.
3. **Carding Forums and Marketplaces:**
    - Online platforms offer a marketplace for buying/selling stolen card data.
    - Cybercriminals exchange information, tools, and resources.
    - Carders often operate in underground communities.
4. **Card Verification Value (CVV) Guessing:**
    - Attackers use algorithms to guess CVV codes.
    - Automated scripts make numerous attempts until a match is found.
    - Successful CVV guesses enable fraudulent transactions.
5. **Card Skimming:**
    - Physical devices (skimmers) are placed on ATMs, gas pumps, etc.
    - Skimmers capture card information during legitimate transactions.
    - Collected data is then used to create counterfeit cards.
6. **Carding via Botnets:**
    - Botnets are networks of compromised computers controlled by attackers.
    - Bots perform automated attacks on e-commerce sites.
    - Botnets execute a high volume of carding transactions rapidly.
7. **Account Takeover (ATO):**
    - Attackers gain access to user accounts on e-commerce platforms.
    - Stolen accounts are used to make purchases with saved card details.
    - Victims' credit card data is exploited for unauthorized transactions.

8. **Refund Fraud:**
    - Fraudsters purchase items with stolen card data.
    - They request refunds to a different account, often a prepaid card.
    - Legitimate merchants unknowingly refund the fraudster.
9. **Drop Shipping:**
    - Attackers use stolen card data to buy items online.
    - Goods are shipped to an intermediary ("drop") address.
    - Fraudsters resell the goods for cash, making it hard to trace.
10. **Gift Card Conversion:**
    - Stolen card data is used to buy gift cards or store credit.
    - Gift cards are sold or traded for cash or other items.
    - Converts stolen credit into usable, less traceable forms.
11. **Triangulation Fraud:**
    - Fraudsters create fake online storefronts.
    - Victim purchases are routed to legitimate e-commerce sites.
    - Attackers collect funds from victims while making it seem legitimate.
12. **Redirection Attacks:**
    - Attackers compromise e-commerce sites and modify payment gateways.
    - During checkout, victims' card data is redirected to attackers.
    - Cybercriminals gain access to sensitive payment information.

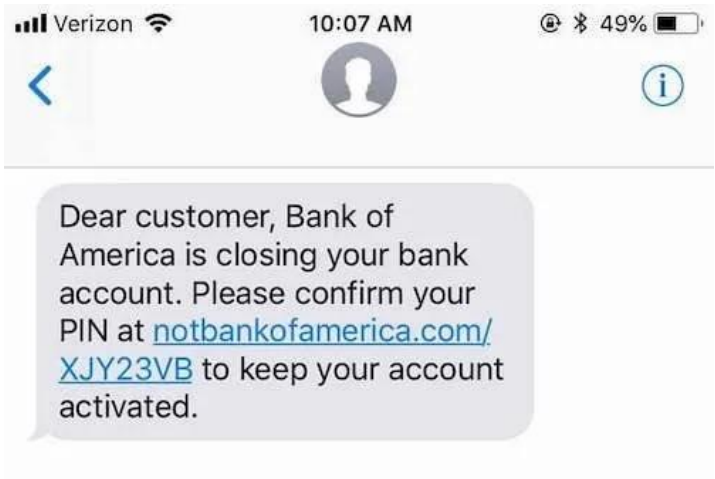
➢ The 9 Most Common Types of Credit Card Fraud in 2022:

1. Scammers buy your credit card account details on the Dark Web

- Due to the number of data breaches in recent years, there's a good chance that scammers can get access to your credit card details on the Dark Web.
- Account details for credit cards with a limit up to $1,000 cost just $150 (and $240 for cards with a limit up to $5,000). While online bank account details go for just $40, according to the Dark Web Price Index.

2. You accidentally give out your details in a phishing email, text, or call

- Phishing is when scammers send emails, texts (called "smishing"), or call you pretending to be from a financial institution, an online account like Netflix, law enforcement, or even the IRS.
- Then, they either ask you to "confirm" your financial information or click on a link that sends you to a fake site that captures your information or downloads malware onto your device.



❖ Smishing text posing as Bank of America, requesting a PIN confirmation via a malicious URL, due to an alleged account closure

- Phishing messages almost always try to force you to act, either through threats or time-limited offers. If something feels off about an interaction, hang up or delete the message and contact the company directly.

3. Your wallet is lost or stolen (aka physical card fraud)

- A stolen wallet can lead to all sorts of fraud.
- With access to your ID and stolen credit card numbers, fraudsters can steal your identity and use it to commit loan fraud or bank fraud. Repairing this situation can be frustrating, expensive, and time-consuming.

4. Fraudsters use "skimmers" and "shimmers" to steal your details at ATMs

- Scammers install small devices into public ATMs in order to "skim" your account details. "Skimmers" work by replacing the magnetic strip reader on an ATM, while "shimmers" work for chip readers.
- If your credit card has an RFID chip, its information could be stolen by someone with a skimming device standing within close proximity to you.
- An even simpler form of this scam is when fraudsters "shoulder surf" your credit card information in public. For example, they might write down your card details as you're using it at a store or watch you enter your information into an online shopping site.

5. An identity thief opens new credit card accounts in your name

- Credit card fraud is identity theft. But in some cases, criminals will skip using your current card details and instead open new cards in your name.
- This is especially dangerous if they also use a change-of-address scam to divert your mail. Not only will they have a card with your name on it, but you won't even get the bill.
- Zoom out: Sign up for a credit monitoring service that alerts you of any suspicious activity. For example, Aura monitors your credit card details, bank accounts, credit score, SSN, online accounts, and more and lets you know if someone is using them without your permission.

6. Someone with access to your card uses it without your permission

- There's an opportunity for fraud anytime your credit card is out in public.
- An unscrupulous waiter could take a picture of your card while settling your bill at a restaurant. Or a store clerk could write down your details while you're not looking. Even leaving your receipt on the counter following a credit transaction could leave a thief with enough information to access your line of credit.

7. Hackers steal your credit card information from online sellers

- Credit card fraud can even happen without your knowledge. Some hackers target e-commerce websites and exploit vulnerabilities to steal massive lists of credit card numbers and information. If you've bought something from one of these stores, they have your info

8. Your financial and personal information is stolen in the mail

- Scammers will dig through your trash or steal your mail in order to get personally identifiable information (PII). If they find credit card statements or pre-approved offers, they can use those to apply for new, fraudulent cards in your name. Or worse, commit identity fraud.

9. "Friendly" fraud from family members or acquaintances

- "Friendly" fraud is a growing problem in the U.S. This is when family members or acquaintances use your credit card without your permission or knowledge. Many financial companies are moving to make "friendly" fraud an official fraud category.

5. Impact and Consequences:

➲ Impacts:

i. **Financial Losses:**
   - Individuals face unauthorized charges, leading to financial strain.
   - Businesses incur losses from chargebacks and refund processes.

ii. **Data Breaches:**
   - Hacking techniques used in carding expose sensitive financial data.
   - Breached data may lead to further cybercrimes beyond carding.

iii. **Reputation Damage:**
   - Companies' reputations suffer due to perceived vulnerability.
   - Loss of customer trust affects long-term brand image.

iv. **Economic Disruption:**
   - Carding-related disruptions can undermine online business stability.
   - Market uncertainty arises from fluctuating consumer confidence.

v. **Innovation Stifling:**
   - Focus on carding prevention diverts resources from innovation.
   - Businesses hesitant to invest in emerging technologies due to security concerns.

vi. **Consumer Confidence Erosion:**
   - Consumers fear using online services due to potential carding risks.
   - E-commerce growth is hindered as customers shift to traditional methods.

vii. **Regulatory Scrutiny:**
   - Regulatory bodies impose fines and penalties for data breaches.
   - Companies must adhere to stricter data protection standards.

viii. **Resource Drain for Law Enforcement:**
   - Law enforcement dedicates time and effort to track and prosecute carders.
   - Limited resources impact their ability to combat other cybercrimes.

ix. **Complex Investigations:**
- Jurisdictional differences complicate cross-border carding investigations.
- Tracing digital footprints requires collaboration between multiple agencies.

x. **Skills Escalation:**
- Carders continuously upgrade hacking skills to evade detection.
- Cybersecurity experts need to enhance skills to counter evolving threats.

➲Consequences:

i. **Legal Action:**
- Perpetrators face criminal charges, including imprisonment.
- Prosecutions act as deterrents for potential carders.

ii. **Financial Industry Costs:**
- Financial institutions bear costs of refunding unauthorized transactions.
- Investment in fraud detection technologies strains financial resources.

iii. **Cybersecurity Advancements:**
- Carding incidents drive innovation in cybersecurity tools.
- Industry focuses on developing more effective fraud prevention measures.

iv. **Identity Theft Surge:**
- Stolen card data enables criminals to commit broader identity theft.
- Victims spend time and resources to recover from identity theft fallout.

v. **Loss of Privacy:**
- Breached personal data exposes individuals to privacy risks.
- Victims may experience social engineering attacks using stolen info.

vi. **Black Market Growth:**
- Underground markets thrive on selling stolen credit card information.
- Carding feeds a cycle of criminal collaboration and data trading.

vii. **Resource Redistribution:**
- Companies allocate funds to bolster cybersecurity infrastructure.
- Budgets are redirected from growth initiatives to protection measures.

viii. **Mitigation Costs:**
- Businesses invest in anti-fraud systems, increasing operational expenses.
- Cost of cybersecurity insurance rises due to carding risks.

ix. **User Education Emphasis:**
- People become more aware of online security practices.
- Companies and institutions offer cybersecurity education to customers.

x. **Global Collaborative Efforts:**
- International law enforcement agencies collaborate to combat carding networks.
- Cross-border cooperation becomes crucial to apprehending carders.

6. Prevention and Mitigation Strategies:

i. **Multi-Factor Authentication (MFA):**
   - Require multiple verification factors for online transactions.
   - Adds an extra layer of security beyond just passwords.

ii. **Encryption of Data:**
   - Encrypt sensitive cardholder data during transmission and storage.
   - Prevents unauthorized access to valuable information.

iii. **Regular Security Audits:**
   - Conduct routine assessments of security systems and processes.
   - Identifies vulnerabilities before they can be exploited.

iv. **User Education:**
   - Educate customers about safe online practices and carding risks.
   - Empower users to recognize phishing attempts and suspicious activities.

v. **Advanced Fraud Detection:**
   - Employ machine learning and AI to identify unusual patterns.
   - Detects anomalies in real-time and blocks potentially fraudulent transactions.

vi. **Tokenization:**
   - Replace actual card data with tokens during transactions.
   - Minimizes exposure of sensitive data, reducing risk.

vii. **Strong Password Policies:**
   - Enforce complex password requirements for user accounts.
   - Reduces the likelihood of unauthorized access to accounts.

viii. **Regular Software Updates:**
   - Keep all software and applications up to date with security patches.
   - Addresses known vulnerabilities that attackers could exploit.

ix. **IP Geolocation and Device Fingerprinting:**
   - Monitor IP addresses and device characteristics for suspicious activity.
   - Helps identify and block fraudulent transactions.

x. **Transaction Velocity Limits:**
   - Set limits on the number of transactions within a certain time frame.
   - Thwarts attempts at mass unauthorized transactions.

xi. **Monitoring Dark Web Activity:**
   - Monitor underground markets for stolen data associated with carding.
   - Allows for early detection and intervention.

xii. **Collaboration with Law Enforcement:**
   - Share information with law enforcement agencies about carding incidents.
   - Aids in tracking down and apprehending carders.

xiii. **Vendor Due Diligence:**
   - Vet and regularly review third-party vendors' security practices.
   - Ensure partners uphold strong security standards.

xiv. **User Account Lockouts:**
   - Implement temporary account lockouts after multiple failed login attempts.
   - Thwarts brute-force attacks on user accounts.

xv. **Real-time Transaction Monitoring:**
   - Monitor transactions in real time to spot and halt suspicious activities.
   - Helps prevent unauthorized transactions before completion.

xvi. **Regular Employee Training:**
   - Train employees to identify and report potential carding attempts.
   - Enhances overall organizational vigilance against cyber threats.

xvii. **Emergency Response Plan:**
   - Develop a comprehensive plan to respond to carding incidents.
   - Ensures a swift and effective response in case of a breach.

xviii. **Data Retention Limits:**
   - Minimize the retention of sensitive card data.
   - Reduces the amount of valuable data that could be compromised.

xix. **Secure Payment Gateways:**
   - Use reputable and secure payment gateways for transactions.
   - Provides an added layer of security for online payments.

xx. Regularly Updated Policies:

- Maintain up-to-date security policies and procedures.
- Reflects changing carding techniques and evolving threats.

7. Case Studies:

1) **Target Data Breach Case Study (2013): -**

- **Introduction:**

  - The Target data breach of 2013 was one of the most significant security breaches in history.
  - Hackers stole 40 million credit and debit records from Target, resulting in an $18.5 million settlement.
  - The breach raised awareness about cybersecurity and brought important lessons for businesses.

- **Details of the Breach:**

  - Occurred during the 2013 holiday season.
  - Stolen records included 40 million credit and debit details and 70 million customer records.
  - High-profile breaches before this incident made customers more cautious.

- **Impact on Customer Trust:**

  - The breach eroded customer confidence in Target's security.
  - Customers feared data leaks and were hesitant to shop at Target.
  - Similar incidents affected companies like Sony PlayStation.

- **Third-Party Involvement:**

  - Attack didn't directly target Target's systems; it started with a third-party vendor.
  - Third-party vendors are often less secure, making them vulnerable entry points.
  - Emphasizes the need for securing all third-party vendors.

- **Target's Response:**

  - Target notified customers about the breach within 20 days and removed the malware.
  - The breach raised concerns about third-party solutions and internal issues.
  - Target implemented more secure chip-and-pin cards.

- **Limitations of Chip-and-Pin:**

  - Chip-and-pin cards added security but couldn't fully prevent breaches.
  - Consumer identities were compromised due to the extensive stolen data.
  - Identity theft was a more significant concern than individual card compromises.

- **Areas for Improvement:**

  - Target's third-party portal vulnerability enabled the breach.
  - Proper network segregation could have minimized the attack's impact.
  - Cybersecurity remains a challenge due to the persistence of cybercriminals.

- **Costs and Impact:**

  - The breach cost Target over $200 million, beyond the settlement.
  - Earnings dropped by 46%, impacting customer trust.
  - Restoring reputation required significant efforts.

- **Lessons Learned:**

  - Prioritize third-party vendor cybersecurity.
  - Swift and transparent response is crucial post-breach.
  - Security measures should address broader impacts.
  - Disaster preparedness plans for breaches are essential.
  - Proactive security audits enhance defence strategies.

- **Protective Measures:**

  - Shift to EMV (chip-and-pin) technology.
  - Thoroughly assess third-party contractors' cybersecurity.
  - Establish premeditated response plans for cyberattacks.

- **Post-Breach Steps:**

  - Cancel affected credit cards and request new ones.
  - Change online passwords with strong combinations.
  - Monitor bank statements and credit reports for unusual activity.
  - Invest in credit monitoring and consider credit freezes.
  - Stay vigilant against phishing and scam emails.

- **Legal Consequences:**

  - Target faced a class-action lawsuit with up to $10,000 per customer settlement.
  - Deadline for claims filing (July 31, 2015) has passed.
  - Payments were made to affected customers with proof of consequences.

- **Identity Theft Concerns:**

  - Stolen data ideal for identity theft: personal details, credit card info, and logins.
  - Vigilance and cybersecurity measures crucial to protect against identity theft.

- **Protecting Yourself:**

  - Use one credit card for retail purchases and monitor statements.
  - Review bank statements and credit reports regularly.
  - Consider credit monitoring and credit freezes.
  - Keep devices updated and use antivirus software.
  - Be cautious of suspicious emails pushing for clicks or downloads.

➢ Conclusion:

- Enduring Lessons: Target breach underscores long-lasting cybersecurity lessons.
- Trust Protection: Breach emphasizes proactive security to safeguard trust.
- Tech Transition: Incident prompts adoption of secure technologies like chip-and-pin.
- Vendor Scrutiny: Third-party scrutiny vital to prevent breaches.
- Comprehensive Response: Robust disaster plans and solutions are essential.
- Beyond Finances: Breach impact extends to reputation and loyalty.
- Collective Defence: Stronger vendor ties, network segregation, and response planning are key.
- Vigilant Approach: Consistent vigilance and adaptable strategies are crucial.
- Blueprint for Security: Target breach guides businesses to fortify defences and prioritize trust.
- Resilience in Action: Proactive measures and adaptation enhance cybersecurity resilience.

2) ShadowCrew Cybercrime Community -

- **Background:**

  - ShadowCrew was an underground online forum and criminal community that operated between August 2002 and November 2004.
  - It played a significant role in facilitating various cybercrimes, including carding, identity theft, and fraud.

- **Origin and Organizational Structure:**

  - The concept of ShadowCrew was developed in early 2002 through discussions between individuals like Brett Johnson (GOllumfun), Seth Sanders (Kidd), and Kim Marvin Taylor (MacGayver).
  - The forum emerged from another underground site, counterfeitlibrary.com, and continued the legacy of facilitating cybercrimes.
  - ShadowCrew hosted sub-forums on hacking, social engineering, credit card fraud, virus development, scams, and phishing.

- **Method and Activities:**

  - ShadowCrew provided a platform for cybercriminals to connect, share information, and collaborate on illegal activities, especially carding.
  - Members engaged in discussions about stealing card data, exploiting vulnerabilities, and conducting fraudulent transactions.
  - The forum facilitated the sale of stolen data, enabling criminals to profit from unauthorized transactions.
  - The site also played a role in drug wholesale trade.

- **Impact:**

  1) Proliferation of Cybercrimes:

     - ShadowCrew's activities extended to various cybercrimes, including identity theft, financial fraud, and unauthorized transactions.

2) Facilitation of Carding:

   - The forum's existence contributed to the growth of the carding ecosystem, making it easier for criminals to access and trade stolen card data.

3) Law Enforcement Action:

   - Law enforcement agencies infiltrated and dismantled ShadowCrew, resulting in multiple arrests, convictions, and legal consequences for members.

4) Learning and Collaboration:

   - Criminals within the community shared knowledge, leading to increased sophistication in cybercrime techniques and activities.

5) Global Nature:

   - ShadowCrew's international membership highlighted the global reach of cybercrime communities and the widespread impact of their activities.

➢ **Aftermath and Legacy:**

- ShadowCrew's structure, marketplace, and review system laid the groundwork for today's cybercrime forums and marketplaces.
- The organization's activities influenced modern scams and computer crimes, shaping the landscape of cybercriminal operations.
- The demise of ShadowCrew was facilitated by law enforcement's collaboration with informants, leading to arrests and convictions.
- The case study showcases the role of law enforcement and the importance of international collaboration in combating organized cybercrime.

➢ **Lessons Learned:**

- The interconnected nature of cybercriminal communities highlights the challenges in combating organized cybercrime.
- Successful dismantling of forums like ShadowCrew underscores the importance of international cooperation among law enforcement agencies.
- Continuous efforts to implement strong cybersecurity measures are essential to protect individuals and organizations from carding-related activities.

➢ **Conclusion:**

1) Underground Cybercrime Facilitation: ShadowCrew served as a prominent example of an underground online forum enabling cybercriminals to connect, collaborate, and engage in various illicit activities, including carding, identity theft, and fraud.
2) Proliferation of Cybercrimes: The forum's existence fuelled a wide range of cybercrimes beyond carding, leading to identity theft, financial fraud, and unauthorized transactions, contributing to the growth of the cybercrime ecosystem.
3) Global Reach and Impact: ShadowCrew's international membership underscored the global nature of cybercrime communities and how their activities affect individuals, organizations, and financial systems on a global scale.
4) Law Enforcement Action: Law enforcement agencies' successful infiltration and dismantling of ShadowCrew, through collaborations and informants, demonstrated the determination to combat organized cybercrime and the need for international cooperation in tackling such threats.
5) Learning and Innovation: Criminals benefited from shared knowledge within the forum, leading to increased sophistication in cybercrime techniques, highlighting the ongoing evolution of cybercriminal tactics.
6) Legacy and Modern Influence: ShadowCrew's impact on the cybercrime landscape continues to be felt through the foundational role it played in shaping the structure, marketplace dynamics, and criminal innovations of today's cybercrime forums and marketplaces.

7) Lessons for Cybersecurity: This case study emphasizes the ongoing necessity for robust cybersecurity measures to counter carding-related activities, as well as the importance of international collaboration and law enforcement efforts to dismantle cybercrime networks.

Also Refer: -

https://web.archive.org/web/20090117135809/http://www.usdoj.gov/usao/nj/press/files/pdffiles/firewallindct1028.pdf#search=%22firewallindct1028.pdf%22

8. Current Trends and Future Outlook:

➲ Current Trends in Carding:

➢ Scam and Phishing Affiliate Programs:

- Cybercriminals are forming partnerships, with a notable rise in scammer collaborations.
- Phishing and scam affiliate programs have gained immense popularity, boasting over 70 such programs in operation.
- Monetary Gains: These programs have proven lucrative, collectively pocketing at least $10 million during the reported period. On average, each participant managed to steal about $83.
- Complex Infrastructure: These affiliate programs have evolved into intricate networks, featuring a strict hierarchy and employing advanced technical setups to automate fraudulent activities.
- Telegram Bots: A notable trend is the extensive use of Telegram bots within these programs. These bots provide participants with ready-to-use scam and phishing materials, enabling the efficient scaling of phishing campaigns.
- Global Expansion: Initially focused on Russia and other CIS countries, these schemes have expanded their online reach to Europe, America, Asia, and the Middle East.
- Brand Impersonation: Scammers have mimicked at least 71 brands from 36 different countries. The phishing websites they create often mimic marketplaces (69.5%), delivery services (17.2%), and carpooling services (12.8%).

➢ Carding Market Trends:

- The carding market witnessed a significant decline of 26% during the review period, decreasing from $1.9 billion to $1.4 billion.
- The closure of Joker's Stash, a notorious card shop, contributed to this decline, resulting in a 17% reduction in the availability of dumps (data stored on card magnetic stripes).
- Dump Price Changes: Interestingly, while the market saw a decrease, the average price of a bank card dump fell from $21.88 to $13.84, with the maximum price increasing from $500 to $750.
- Rise in Text Data Market: Conversely, the market for the sale of bank card text data (card numbers, expiration dates, owner names, addresses, CVVs) surged by 36%.
- Reasons for Growth: This growth can be attributed to the proliferation of phishing websites that impersonate well-known brands, particularly during the pandemic.
- Text Data Price Changes: The average price for text data increased from $12.78 to $15.2, while the maximum price skyrocketed seven-fold, reaching an unprecedented $1,000.

These trends in cybercrime highlight the evolving landscape, with scammers actively partnering to execute fraudulent schemes, while the carding market experiences shifts driven by the closure of prominent card shops and the rise of phishing websites impersonating popular brands.

➲ Future Outlook in Carding and Online Fraud:

1. **E-commerce Growth and Credit Cards:**
    - E-commerce is on a rapid growth trajectory, with credit cards becoming increasingly popular.
    - Predicted Market Size: The global digital credit card market is projected to reach a staggering $724.3 billion by 2028, showcasing the immense opportunity for fraud in this sector.
2. **Escalating Online Fraud:**
    - As e-commerce expands, online fraud becomes more enticing for organized criminal groups and carders.
    - Alarming Statistics: The Federal Trade Commission (FTC) reported $148 million in fraud-related credit card losses in just the first nine months of 2021.
    - Combined Losses: When considering debit card fraud alongside credit card fraud, the cumulative losses amount to substantial financial damage.
3. **Heightened Cybercriminal Sophistication:**
    - With a larger target audience, cybercriminals are upping their tactics and sophistication.
    - Advanced Bots: Security researchers are uncovering increasingly sophisticated bots capable of mimicking human behavior with remarkable accuracy.
    - Evading Detection: These advanced bots pose a challenge for traditional security technologies, making fraud detection more difficult.
4. **Consumer Vulnerability:**
    - Consumers are at risk as cybercriminals adapt and refine their strategies.
    - Escalating Losses: The data from the FTC highlights a concerning trend; consumers reported $148 million in credit card-related scams

in just the first nine months of 2021, surpassing the total for all of 2020.

- Credit Card Scams on the Rise: Nearly 40,000 consumers reported falling victim to scams involving credit card payments during this period.

5. **Targeted Impersonation:**
    - Scammers frequently impersonate well-known companies or government agencies.
    - Target Credit Cards in Focus: A notable development is the emergence of Target credit cards as scammers' preferred choice. They accounted for approximately $35 million in payments to scammers, surpassing all other brands.
    - Higher Median Loss: The median loss reported by consumers when using Target credit cards was $2,500, higher than any other brand. Nearly a third reported losses exceeding $5,000.
6. **Changing Scammer Tactics:**
    - Scammers instruct consumers to purchase credit cards, often from Target stores, more frequently than any other location.
7. **Steady Rise in Credit Card Scams:**
    - Since 2018, both the number of consumers reporting credit card-related scams and the reported losses have consistently increased.
    - Median Reported Loss: The median reported loss to scammers when using credit cards has risen from $700 to $1,000 over time.
8. **Consumer Awareness and Protection:**
    - As credit card scams and online fraud continue to evolve, consumer awareness and protection measures become vital.
    - Education: Educating consumers about potential scams and emphasizing caution when using credit cards is essential.
    - Enhanced Security: Organizations and retailers must strengthen security measures to protect consumers from falling victim to scams.

9. Conclusion on Carding:

1. **Increased Complexity and Challenges:**
    - The carding ecosystem has evolved, becoming more intricate and less appealing for cybercriminals.
    - What was once a simple endeavour has transformed into a multistage operation with multiple entry barriers and potential points of failure.
2. **Law Enforcement Operations:**
    - Law enforcement agencies have escalated their efforts to target carders, increasing the risks associated with this criminal activity.
3. **Profitability Under Question:**
    - The decreasing validity rates of stolen card data have raised doubts about the profitability of carding operations.
4. **Continued Demand and Resilience:**
    - Despite these challenges, the "death of carding" is not imminent. New carding shops frequently emerge, indicating that there is still demand for stolen card data.
    - Some threat actors believe there are opportunities to profit from this type of cybercrime.
5. **Adaptation and Creativity:**
    - Cybercriminals are demonstrating creativity by relying on coding and operating their own skimmers, finding innovative ways to adapt and sustain carding activities.
6. **Consumer and Financial Vigilance:**
    - Financial services organizations and individual consumers must remain vigilant against the persistent threat of carding.
    - As carders' tactics and techniques continue to evolve, staying informed and implementing robust security measures is crucial.

7. **Market:**

- Desperation may still drive sales in the carding market, with individuals seeking opportunities to make illicit gains.
- The emergence of new carding shops and the adaptability of cybercriminals highlight the ongoing relevance of carding as a cyber threat in 2023 and beyond.

8. **Underlying Demand Persists:**

- The underlying demand for stolen card data remains persistent, driven by individuals seeking financial gains through fraudulent activities.

9. **Global Reach and Expansion:**

- Carding operations are not limited by geographical boundaries; they have expanded their reach from traditional markets to new regions, making it a global concern.

10. **Collaborative Threat Landscape:**

- The carding ecosystem demonstrates a collaborative threat landscape, with threat actors often working together in affiliate programs, indicating the adaptability and resilience of cybercriminal networks.

10. References:

3) ChatGPT
4) Google Dorks
5) Wikipedia
6) web.archive.org
7) www.idstrong.com
8) www.quora.com
9) www.reliaquest.com
10) https://www.reportlinker.com/p06412029/Global-Digital-Gift-Card-Market-Size-Share-Industry-Trends-Analysis-Report-By-Functional-Attribute-By-End-User-By-Application-By-Regional-Outlook-and-Forecast.html?
11) www.ftc.gov
12) https://www.analyticsinsight.net/the-threat-of-misusing-stolen-card-data-an-introduction-to-carding-attacks/

11. Carding Tools:

A. https://github.com/Baiiki/credit-card-generator
B. https://github.com/astros3x/Astri
C. https://github.com/hakanonymos/paypal_integration_carding
D. https://github.com/oldnum/cardesc
E. https://github.com/rimurx/DemonLordV2
F. https://github.com/Unavailable072/carding

12. Carding Websites:

A. https://cardgenerator.io/
B. https://www.duplichecker.com/credit-card-generator.php
C. https://smallseotools.com/credit-card-generator/
D. https://neapay.com/online-tools/credit-card-number-generator-validator.html
E. https://bankomat.cc/
F. https://batmarketcc.cc/

-------END-------