Carding là gì ?

Carding là hình thức gian lận thẻ thanh toán quốc tế, sử dụng thông tin thẻ bị đánh cắp để thanh toán các giao dịch hoặc mua sắm trái phép

Thông tin thẻ bị đánh cắp thường được lấy thông qua các phương thức như:

👉 giả mạo email (phishing)

👉 rò rỉ dữ liệu (data breaches)

👉 phần mềm độc hại (malware)

👉 hoặc chợ đen trên dark web

Các hình thức khai thác Carding

- Mua hàng trái phép

Kẻ gian dùng thông tin thẻ bị đánh cắp để mua các mặt hàng đắt tiền như:

→ thiết bị điện tử, quần áo, hoặc thẻ quà tặng.

- Bán lại hàng hóa đánh cắp

→ Các sản phẩm mua bằng thẻ đánh cắp thường được bán lại để lấy tiền mặt.

- Tạo tài khoản/thẻ giả

→ Các giao dịch bằng thẻ đánh cắp có thể được dùng để tạo danh tính và tài khoản giả, phục vụ cho các hoạt động lừa đảo khác.

- Gian lận đăng ký dịch vụ

→ Tội phạm sử dụng thẻ bị đánh cắp để đăng ký các dịch vụ trả phí, ví dụ như:

→ nền tảng xem phim trực tuyến hoặc khóa học online.

Có thể tổng hợp lại thành 3 dạng:

- Pay in-app: Khai thác thông qua các gói ứng dụng như nạp game,gói coin donate,các gói nâng cấp …

Lợi nhuận thu được từ 20-30%

- Checkout: Khai thác thông qua việc mua sắm các hàng hòa đắt tiền trên các sàn như amazon,ebay …

Lợi nhuận thu được từ 50-60%

- Cashout: Rút tiền trực tiếp như nạp tiền ví crypto, gán thẻ giả …

Lợi nhuận thu được từ >80%

VD: Thẻ tín dụng có 1000 USD thì Pay in-app thu được 300 USD , Checkout 600 USD và Cashout 800 USD

1. Các loại thẻ thanh toán quốc tế:

VISA CARD	MASTER CARD	AMEX
4XXX XXXX XXXX XXXX	5500 XXXX XXXX XXXX	34XX XXXXXX XXXXX
16 số	16 số	15 số
	Các dải số: 51-55,2221-2720	Các đầu số: 34,37

Ngoài ra còn có các tổ chức phát hành như:

Discover: đầu số 6011,65,dải số 644-649

JCB: dải số 3528-3589

UnionPay: đầu số 64

Diners Club: đầu số 36,38,39

2. Phân loại theo chức năng tài chính

Credit (Tín dụng) : Dùng tiền của ngân hàng, thanh toán trước – trả sau

Debit (Ghi nợ) : Dùng tiền có sẵn trong tài khoản ngân hang

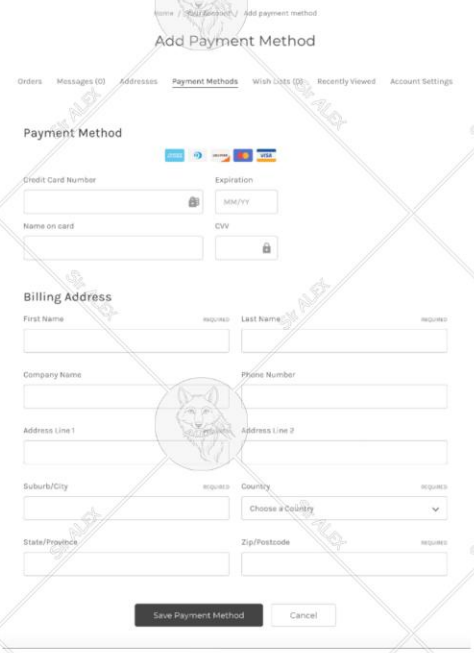
Prepaid (Trả trước) : Nạp tiền trước, chỉ tiêu trong số tiền nạp

Virtual (Thẻ ảo) : Là phiên bản online của thẻ thật – dùng để thanh toán online

Thẻ được khai thác nhiều nhất là Credit và Debit còn Prepaid thì ít vì tỉ lệ có số dư thấp, còn Virtual thì bảo mật cao và gặp nhiều hạn chế thanh toán

CC/Ci là gì ?

CC hay Ci là một thuật ngữ thường được sử dụng trong **Black MMO/Black UG**, nhằm chỉ một **bộ dữ liệu đầy đủ thông tin thẻ thanh toán quốc tế**. Những thông tin này thường bao gồm:



- **Số thẻ tín dụng/PAN:** xxxx xxxx xxxx xxxx
- **Tên chủ thẻ/NAME:** Abc
- **Ngày hết hạn/DATE:** xy/xz
- **Mã bảo mật CVV/CVC:** abc
- **Địa chỉ thanh toán (Billing address):** xxxx
- **Số điện thoại:** 999999999xx
- **Email:** xyz@gamil.com

Ngoài ra, đôi khi còn bao gồm:

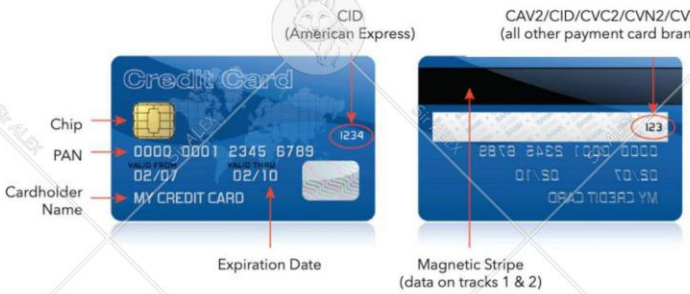
- **Số an sinh xã hội (SSN)**
- **Thông tin đăng nhập tài khoản ngân hàng**

Ci thường được chia thành các dạng:

- Ci Non: Gồm thông tin số thẻ (PAN) – Ngày hết hạn – Mã bảo mật CVV
  Ci Non thường được dùng để check Ci xem sống/chết, spam gateway, test sandbox … không dùng để thanh toán thực tế được
- Ci Full: Gồm tất cả thông tin cần để thanh toán
  PAN|Date|CVV|NAME|Địa chỉ|ZIP Code|Email/SĐT
  Ci full thường được sử dụng cho Pay In-App thanh toán các item không cần OTP
  Ví dụ:
  4232232160995735|01/28|533|Cindy Sttoud|62 Vires Road|London|KY|40744|US|(270) 350-0763|stroudsdanes@yahoo.com|| => VISA|DEBIT|USD
- Ci Full True: Gồm tất cả thông tin như Ci Full còn cần thêm IP address, User – Agent và có giao dịch online
  Ci Full True được dùng vào các giao dịch cao >100$ cần OTP nên cần, Ci đã từng giao dịch online để hệ thống dễ approve ngoài ra sử dụng thông tin IP + User – Agent để fake đúng fingerprint để trông giống thật nhất tránh kích hoạt OTP
- Ci Full True Autopay: Hàng cao cấp không yêu cầu OTP hoặc 3DSecure , cái cần là chỉ cần Giả IP + UA + Browser tốt thì hoạt động như thật. Có khi còn mua được cả hàng đủ thông tin để cashout như người chủ thẻ.
- Ví dụ về thông tin của Ci Full True –>

Card Number: 5463255098297848
Expiry Date: 09/27
CVV2: 381
Type: MASTERCARD
Debit/Credit: CREDIT
Subtype: N/A
Cardholder Name: JERRY L UITERMARKT
Country Code: US
State: IA
City: Pella
ZIP: 50219
Address: 807 North Hwy T15
Phone: 6417800327
E-Mail: jmuitermarkt@yahoo.com
Extra Info: N/A
DOB: N/A
SSN: N/A
MMN: N/A
AT&T PIN: N/A
ATM PIN: N/A
OTP: N/A
IP address: 98.97.15.47
Email password: N/A
Driver License: N/A
Last Paid Amount: USD: 31.75
User-Agent: Mozilla/5.0 (iPhone CPU iPhone OS 18_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.5 Mobile/15E148 Safari/604.1
Purchase Date: 2025-07-26 04:22

BIN là gì?



6-8 số đầu tiên của số PAN gọi là BIN: Đây là phần quan trọng để xác định ngân hàng phát hành, quốc gia, loại thẻ, và khả năng thanh toán...

Để check những thông tin cơ bản như trên có thể sử dụng các web: bins.su,bincheck.io...
nhưng ngoài những thông tin đó có 2 thông tin quan trọng hơn cần check là VBV và AVS cần sử dụng tool hoặc các bot check mất phí.

Vậy những thông tin có được có tác dụng gì?

- Nhà phát hành: VISA, MasterCard,Amex... chủ yếu là xác định thẻ quốc tế hay nội địa (thẻ quốc tế thì dễ xài, nội địa thì khai thác tùy năng lực)
- Bank phát hành: Bank có bank dễ khai thác có bank khó (VD bank nhỏ ở một số quốc gia nhỏ như Mỹ-Latinh, châu Phi dễ khai thác vì bảo mật kém hơn..)
- Quốc gia phát hành: Một số app yêu cầu thanh toán giới hạn một số quốc gia nhất định
- Loại thẻ: Debit, Credit, Prepaid..(Credit thì dễ có nhiều tiền để khai thác hơn..)
- Level: Phân loại mức độ và mục đích sử dụng của thẻ
  + Traditional/Classic/Consumer/Personal: Thẻ thường gặp phát hành cho cá nhân
  + Business: Thẻ cho doanh nghiệp ,hạn mức cao, độ trust cao, bảo mật thường dễ hơn...
  + Enhanced: Cá nhân cao cấp hoặc doanh nghiệp nhỏ, nhiều tiền, trust cao
  + Government: Thẻ chính phủ, gặp thì né cho lẹ dù ở đâu cũng tốt nhất không tham làm gì
  ..... ngoài ra còn nhiều level nữa

Những thông tin này đều có thể check được miễn phí. Cơ bản là có thể xác định để tìm kiếm được BIN có bảo mật thấp khai thác dễ phù hợp với gateway.

Ngoài ra còn 2 thông tin vô cùng quan trọng là VBV và AVS

VBV là gì

Trước tiên giải đáp về 3D Secure: Là lớp xác minh bổ sung khi thanh toán online bằng thẻ thanh toán quốc tế.Khi bật 3DS, bạn sẽ gặp thêm một bước như:

→ Nhập mã OTP gửi về điện thoại,

→ Hoặc nhập mật khẩu tĩnh, PIN, hoặc xác minh sinh trắc học.

Mỗi tổ chức phát hành có tên gọi khác nhau nhưng qua tool check đều trả về thông tin (**Non VBV: Yes/No)**

Tương ứng đầu bin đó khi thanh toán có yêu cầu OTP hay là không

BIN/IIN	411177
Thẻ thương hiệu	VISA
Loại thẻ	DEBIT
Cấp thẻ	PREPAID CORPORATE T&E
Tên nhà phát hành / Ngân hàng	INDUSIND BANK, LTD.
Trang web của Nhà phát hành / Ngân hàng	------
Nhà phát hành / Điện thoại ngân hàng	------
Tên quốc gia ISO	INDIA
Lá cờ Tổ quốc	
Mã quốc gia ISO A2	IN
Mã quốc gia ISO A3	IND
Tiền tệ quốc gia ISO	INR

AVS là gì

AVS là hệ thống kiểm tra **sự khớp giữa billing address (địa chỉ thanh toán)** và **địa chỉ đã đăng ký với ngân hàng**. Dựa vào ZIP code, Street Number, để xác định độ chính xác của giao dịch

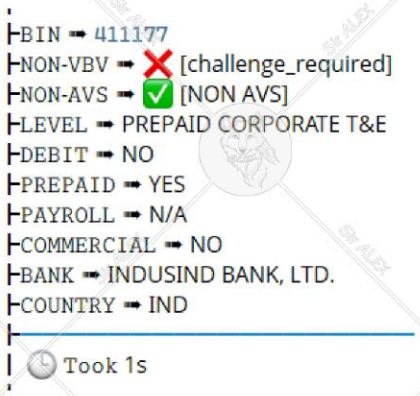
Kết luận lại là :

VBV: No – AVS: No -> Bảo mật cực thấp dễ khai thác

VBV: Yes (no OTP) – AVS: Yes -> Có lớp bảo vệ nhẹ, yêu cầu ci cần đúng address

VBV: Yes (OTP) – AVS: Strict -> Rất bảo mật, dùng được nếu có CI full true

Nhưng mà những Bin ngon thì đa phần đều có VBV còn AVS thì tùy theo khu vực



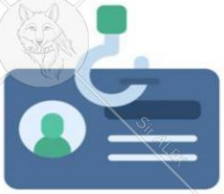
Để tìm ra bin ngon chỉ có cách sử dụng tool để gen và test rất nhiều thời gian công sức tiền bạc để tìm ra được đầu bin ngon để làm thường thì các tay to tìm ra được đầu bin tốt sẽ tìm mua hết các ci trên thị trường đầu bin đó về để làm dần tới khi nào hết hoặc nhà phát hành hoặc bank phát hiện ra lỗ hổng bị khai thác sẽ fix lại.

Đầu BIN rất quan trọng giống như bán hàng có được sản phẩm win vậy

Còn làm sao để test được đầu BIN ngon và các tool để sử dụng sẽ được dạy sau.

Làm sao để có Ci

CC Dumping



CC Phishing

Spaming

1. **CC Dumping:**
   Lấy trộm thông tin thông qua dải từ của thẻ vật lý
   - Skimmer cài ở ATM hoặc POS cà thẻ
   - Malware POS cài trong máy thanh toán cửa hang
   - Hack hệ thống POS
2. **CC Phising:**
   Lừa người dùng tự cung cấp thông tin qua các trang web giả mạo,email,SMS...
3. **Scan/spaming:**
   Dùng tool quét thông tin thanh toán của người dùng bị lộ khi giao dịch online .... Sau đó dùng tool để Spam tìm ra thẻ sống/có giá trị thanh toán

3 cách đó là 3 dạng thông dụng mà hacker dùng để lấy Ci, nhưng mà thường thì hacker lấy Ci cũng sẽ bán ra chứ không khai thác. Lý do thì cơ bản tay to không ăn tiền lẻ, ăn từ gốc tới ngọn dễ bị truy vết ...

Vậy thì với anh em thì không cần quan tâm mấy cái này chỉ cần biết đi mua về khai thác là đủ rồi:

CC Shops

CC Seller

1. **Darkweb Market:**

Ưu điểm: Lượng hàng lớn đa dạng, hàng đảm bảo cơ bản giống mô tả, nhiều hàng ngon fresh ...

Nhược điểm: Đăng ký tài khoản cần nhiều bước kyc, kích hoạt tài khoản luôn cần 1 số tiền để kích hoạt tài khoản thường từ 50-100$. Các site thường hay bị đánh sập nên thường xuyên thay đổi miền khiến người mua đôi khi bị lừa vào site fake, không có bảo hành

2. **Seller:**

Ưu điểm: Rẻ thích hợp để mua số lượng lớn, giao dịch nhanh, có bảo hành đổi trả các kiểu

Nhược điểm: Seller không uy tín thì bị scam vì giao dịch ug không có người nhận trung gian. Thường là dựa vào có người giới thiệu hoặc test giao dịch nhỏ.

Hàng thì hay bị xào hàng cũ với hàng mới để tăng số lượng

Hàng không đa dạng đôi khi không mua được hàng mình cần phải chờ

Bypass detection

Mục tiêu của bypass detection thiết bị là để đánh lừa hệ thống tin rằng:

- Thiết bị là "người dùng thật", không phải bot/spoof.
- CI được dùng từ thiết bị hợp lệ và quen thuộc.
- Không có dấu hiệu "dùng thẻ từ thiết bị lạ" → tránh bị khóa, yêu cầu OTP hoặc từ chối.

Một số thông tin cần bypass:

- Fingerprint: Làm mới, làm sạch thiết bị để không nằm nằm blacklist hoặc làm sao cho thiết bị giống với chủ thẻ dùng
  + Phone: Hệ điều hành, model, IMEI / MEID / Serial, ẩn Root / Jailbreak
  + PC: User-Agent, Screen Resolution, Cookie/LocalStorage
- Time zone/Language: Theo địa chỉ trên CI hãy cài ngày giờ và ngôn ngữ theo thông tin địa chỉ đó
  Chủ thẻ vẫn đang sử dụng thẻ của họ.
  Họ không thể "dịch chuyển tức thời" qua nhiều múi giờ trong vài phút được.
  Nếu hệ thống phát hiện có người dùng thẻ ở múi giờ khác chỉ vài phút sau khi họ vừa giao dịch ở một nơi khác, thì sẽ bị nghi ngờ ngay.

- IP: Tương tự timezone thì IP cũng cần phải fake sao cho gần với địa chỉ nhất
  + VPN: dùng VPN cũng được thôi nhưng chỉ qua mặt được các trang bảo mật thấp như DoorDash thôi còn như trang BestBuy chẳng hạn thì bị phát hiện ngay
  Lý do:
  VPN sử dụng địa chỉ IP chia sẻ (shared IP)
  → Nghĩa là nhiều người khác cũng đang dùng chung IP với bạn.
  Một số website lớn đã bắt đầu theo dõi và nhận diện các IP đó,
  → Và ghi nhận lại hành vi đã từng được thực hiện bằng IP đó.
  + Proxy: Sử dụng proxy SOCKS5 là OK nhất vì SOCKS5 có thể chọn vị trí chính xác nhất (tới tận mã ZIP code) và quan trọng là chỉ duy nhất mình sử dụng (nếu mua được nguồn uy tín)

IP có lưu ý quan trọng đó là Black list:

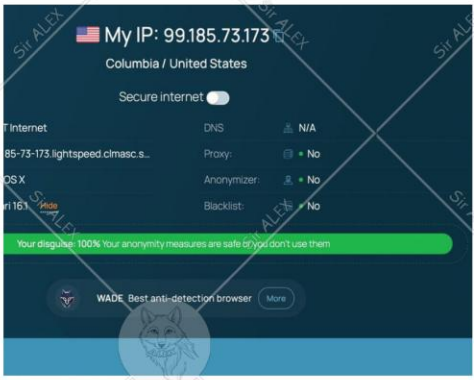
Khi IP của bạn bị đưa vào blacklist (danh sách đen)

Khi IP của bạn bị blacklist, điều đó có nghĩa là các trang web từng gặp IP đó trước đây,

và ai đó đã gây ra rắc rối nghiêm trọng với IP đó.

Việc IP bạn bị blacklist không có nghĩa là không thể carding được nữa,

→ nhưng nó sẽ làm giảm khả năng thành công của bạn khoảng 30%.



Whoer.net là một trang khá hay — nó có thể cho bạn biết IP của bạn có bị blacklist hay không.

Nhưng t không dùng nó để kiểm tra blacklist.

→ T chỉ dùng nó để kiểm tra tổng thể độ "ẩn danh" và độ mạnh của kết nối của mình.

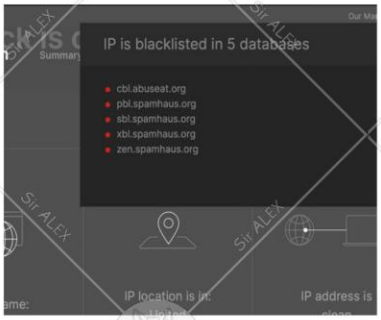
Trang này có thể cho bạn biết nếu: Múi giờ bị lệch hoặc có thông số nào đó trong thiết lập đang làm lộ danh tính của bạn và thậm chí gợi ý nên chỉnh sửa lại điểm nào để trở nên ẩn danh hơn.

Về kiểm tra blacklist IP

Với việc kiểm tra blacklist, tôi khuyên bạn dùng trang: Pixelscan.net/ip

👉 Trang này không chỉ cho bạn biết IP có bị blacklist hay không,

mà còn chỉ rõ những website hoặc dịch vụ nào đã đưa IP đó vào danh sách đen.



Về blacklist từ spamhaus.org:

Blacklists từ Spamhaus thì thường có thể bỏ qua,vì hầu hết IP đều bị dính vào danh sách của họ.

Nếu IP của bạn bị blacklist mà không phải do Spamhaus, thì IP bạn có vấn đề rồi

Nếu IP của bạn bị blacklist trên Whoer

→ thì toàn bộ quá trình sẽ không hoạt động đâu.

Điều gì xảy ra khi bị một trang web blacklist giao dịch của bạn?

Trang đó sẽ gửi báo cáo cho công ty phát hành thẻ và tạm khóa thẻ của bạn

Sau đó, họ sẽ liên hệ với chủ thẻ để xác minh xem giao dịch đó có phải do họ thực hiện không

DNS Leak

Hãy tưởng tượng kết nối VPN hoặc Proxy của bạn giống như việc gửi một bức thư:

Bên trong bức thư là IP thật của bạn

Bạn bỏ nó vào một phong bì, rồi ghi bên ngoài là địa chỉ giả (IP giả) — tức là địa chỉ mà bạn đang "ngụy trang"

DNS leak là gì?

Một DNS leak giống như việc IP thật của bạn vô tình bị lộ ra ngoài phong bì.

Giống như phong bì bị trong suốt — khiến người khác nhìn thấy bạn thực sự là ai.

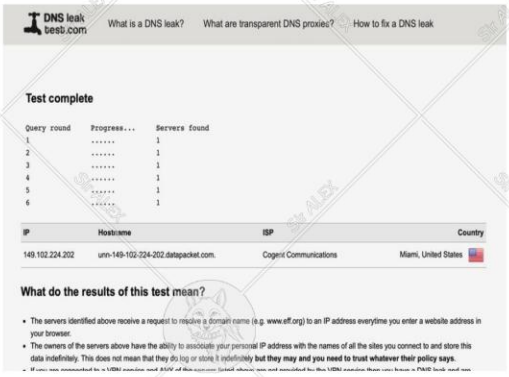
→ Mặc dù bạn đang cố giấu thông tin, máy tính vẫn có thể vô tình tiết lộ website bạn đang truy cập.

Cách kiểm tra DNS Leak bằng dnsleaktest.com

Chạy bài kiểm tra mở rộng (Extended Test)

Hãy chọn "Extended Test" trên dnsleaktest.com

Bài test chỉ mất vài giây, và **kết quả lý tưởng là chỉ có 1 địa chỉ IP hiển thị.



Nhưng nếu:

Có 2 hoặc 3 IP → Chưa phải quá tệ, có thể vẫn ổn tùy vào thiết lập

Từ 4 IP trở lên → Rất tệ, nghĩa là DNS đang bị rò rỉ nghiêm trọng

❗ Nếu kết quả quá tệ?

→ Có khả năng là ai đó chưa flush DNS trước khi kết nối.

Việc này khiến DNS cũ vẫn lưu trên hệ thống và lộ ra dù bạn đã bật VPN hoặc proxy.

Cách fix

PC: mở "Command Prompt", nhập lệnh "ipconfig /flushdns"

Nếu thành công, bạn sẽ thấy thông báo:

Successfully flushed the DNS Resolver Cache

Phone: Dùng app đổi DNS như Intra, DNS Changer