다크웹과 신용카드 보안 위협

IT정보공학과 김아은

INDEX

다크웹과 신용카드 보안 위협

신용카드 보안 위협 동향

💳 신용카드 이용 현황

- 국내 소비자들의 신용카드 이용 실적은 지속적으로 증가하였고, 이용액 역시 증가하는 추이를 보임

  (금융감독원)

  - 21년말 기준 **신용카드 발급매수**(누적)는 **1억 1,769만매**로 전년말(1억 1,373만매) 대비 **396만매(+3.5%) 증가**
  - 21년 중 **신용카드 이용액**은 **779.0조원**으로 전년(705.3조원) 대비 **73.7조원(+10.4%) 증가**

- 신용카드는 이용의 편리성을 가장 큰 장점으로 내세워 지난 수십 년간 주로 사용되던 현금을 대체해왔다.

→ 새로운 지급 수단이 갖고 있는 민감한 정보를 외부의 위협으로부터 보호해야 할 필요성 대두

신용카드 보안 위협 동향

카드 결제에 사용되는 주요 정보

- 신용카드를 이용한 결제는 온라인 결제와 오프라인 결제로 구분됨

구분	사용 정보
온라인 결제	카드번호, 유효기간, 보안코드(CVC, CVV 등)
오프라인 결제	트랙2(카드번호 + 유효기간, 서비스코드, 카드 인증번호)

신용카드 보안 위협 동향

카드 결제에 사용되는 주요 정보

온라인 결제	카드번호, 유효기간, 보안코드(CVC, CVV 등)

신용카드 보안 위협 동향

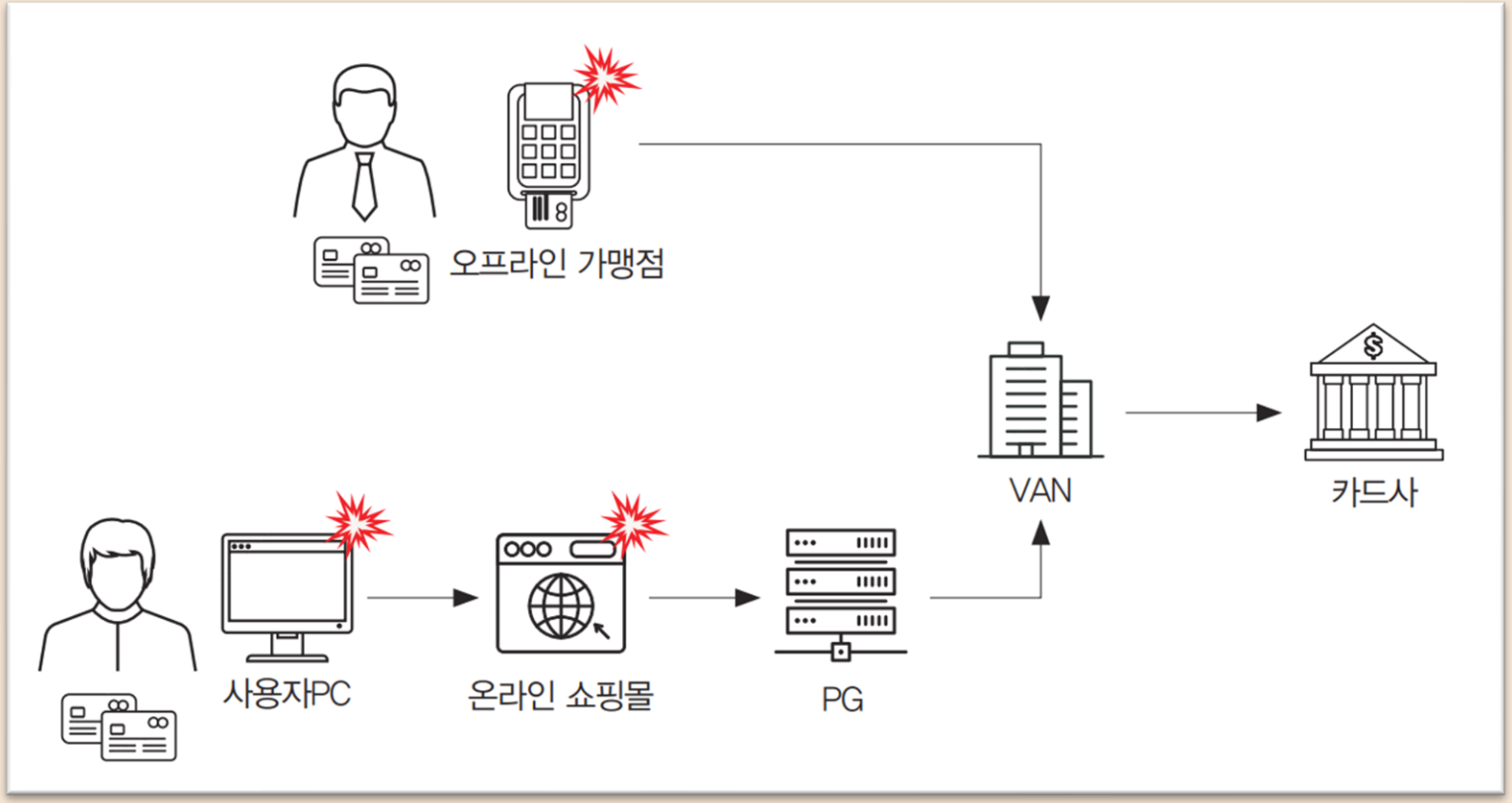
카드 결제에 사용되는 주요 정보

오프라인 결제	트랙2(카드번호 + 유효기간, 서비스코드, 카드 인증번호)

타입	최대 길이	용도	주요 포함 정보
Track1	79 byte	포인트카드 등	이름, 유효기간, 서비스코드 등
Track2	**40 byte**	**신용카드**	**유효기간, 서비스코드 등**
Track3	109 byte	현금카드	국가코드, 통화 단위 등

신용카드 보안 위협 동향

신용카드 거래 프로세스 내 주요 침해 구간



신용카드 보안 위협 동향

신용카드 정보 탈취 목적

- 탈취되는 다양한 고객 정보들은 암시장에 판매하거나 2차 공격에 활용
- 신용카드 정보는 판매 뿐만 아니라 복제카드를 제작하여 부정 결제 또는 부정 인출에 활용 가능 → 가치가 높은 정보

- 탈취한 신용카드 정보를 판매하기 위한 채널로 익명성이 보장된 다크웹에서 암시장이 형성됨

신용카드 보안 위협 동향

💳 신용카드 유출 사고 피해

1) 카드사 및 피해 기업

- 유출이 확인된 신용카드의 재발급 비용 (카드 1장당 3000~6000원 → 100만건 유출 시 최대 60억 원의 비용 소요)
- 카드 정보가 유출된 고객들의 집단소송에 의한 비용 (2014년 국내 카드 3사의 카드정보 유출 사건의 소송 규모 257억 8100만원)
- 피해 기업의 이미지에 부정적인 영향 → 장기적으로 상당한 손실 예상

2) 고객

- 카드 부정 사용에 의한 피해 금액의 경우, 카드사에서 전액 보상하므로 고객의 금전적인 손실까지는 이루어지지 않음
- 실제 보상까지는 최대 한 달까지 소요되는 불편함, 기존에 신청했던 공과금 자동 결제 계좌를 변경 필요,
  재발급 전까지 당장 필요한 경우에도 사용할 수 없음

신용카드 보안 위협 동향

💳 신용카드 유출 방지 및 유출 카드 대응

1) IC카드 적용

- IC 카드란 마이크로프로세서, 카드 운영체제, 보안 모듈, 메모리 등을 갖춘 IC(Integrated Circuit)칩을 카드에 내장하여, 기존의 마그네틱 카드에 비해 보안성이 대폭 향상된 카드
- 국내의 POS 단말기 → 대부분 보안 수준이 강화된 방식을 사용하여 마그네틱 결제 방식도 카드 정보를 보호
  보안 수준이 낮은 해외 가맹점 → 마그네틱 방식으로 결제 시 카드 정보의 유출 위협은 여전히 존재함

신용카드 보안 위협 동향

💳 **신용카드 유출 방지 및 유출 카드 대응**

2) POS 단말기 보안 강화

- POS 단말기에 존재하는 구조적인 취약점을 보완하기 위해
  기존의 취약한 마그네틱 방식의 리더기에서 **IC 방식의 리더기로 교체**
- 하지만 아직까지는 IC 칩 방식과 마그네틱 방식을 모두 사용 중
  → IC 칩으로 결제되지 않는 경우를 대비
  → 신용카드 정보가 즉시 암호화되고, 메모리나 디스크 등에 저장하지 않도록 보안성 강화

신용카드 보안 위협 동향

💳 신용카드 유출 방지 및 유출 카드 대응

3) 이상거래탐지시스템(FDS) 운영

- 이상거래탐지시스템(Fraud Detection System)은
  기존과 다른 패턴의 수상한 금융거래를 탐지하는 시스템을 개발해 적용한 것
- 금융보안원, 국내 금융회사에서 카드 결제, 계좌이체 등 전자금융거래에서 발생하는 거래 유형을 분석하여
  이상금융거래를 탐지 및 차단하는 중

신용카드 보안 위협 동향

💳 신용카드 유출 방지 및 유출 카드 대응

4) 카드 부정사용 예방 서비스

- 국내 카드사에서는 고객의 카드가 해외에서 부정 사용되는 것을 막기 위해 다양한 부가 서비스를 운영
- ex) 고객의 신용카드가 해외에서 사용되는 것을 원천적으로 막거나
  해외에서 거래 발생 시 출입국 관리 사무소를 통해 고객의 출입국 유무를 확인하여 승인을 진행
- 이러한 예방 서비스는 고객이 직접 신청해야 하기 때문에 모든 부정 사용을 사전에 예방하기에는 어려움

신용카드를 노리는 위협그룹 및 악성코드

공격 그룹

- 현재까지 보안 분석가에 의해 발견되고 명명된 위협그룹은 300여개가 넘으며 주로 금융, 에너지, 정부 기관, 커머스 등을 타겟으로 활발히 활동하고 있다.

신용카드를 노리는 위협그룹 및 악성코드

공격 그룹

공격 그룹	공격 방식
FIN6	• 카드 정보를 탈취하여 수익을 창출하는 공격 그룹 • POS 단말기에 악성코드 감염 → e-커머스의 결제 웹페이지에 e-skimming 악성코드 활용 • 탈취한 카드 정보는 카딩샵에 판매
FIN7	• 금융 정보를 타겟으로 활발하게 활동한 공격 그룹 • 초기 침투는 악성코드를 포함한 피싱 메일로 공격하며, POS 악성코드 사용 • 침투 및 공격에는 CARBANAK 악성코드 사용하며 최근에는 RYUK 랜섬웨어 유포
FIN8	• 스피어 피싱, 제로데이 익스플로잇, POS 단말기의 카드 정보 탈취 등의 다양한 공격 벡터 활용 • 지속 실행과 정보 수집을 위해 BADHATCH 악성코드 활용 • PUNCHBUGGY 다운로더와 PUNCHTRACK RAM-스크래핑 악성코드 활용

신용카드를 노리는 위협그룹 및 악성코드

공격 그룹

공격 그룹	공격 방식
FIN11	• POS 악성코드 및 랜섬웨어 유포 공격을 통해 금전적 이득을 노리는 공격 그룹 • 주로 피싱 메일을 이용해 공격 대상 네트워크에 침투 • 광범위하고 다양한 악성코드 셋을 사용
MageCart	• e-커머스 사이트에 침투해 신용카드 정보를 탈취하는 위협 그룹 • e-커머스 상의 카드 결제를 수행하는 웹 페이지에 악성 스크립트를 삽입하여 결제 정보를 탈취 후 C2 서버로 전송 • 탈취한 카드 정보는 다크웹 내 러시아어로 제작된 카딩샵에서 유통

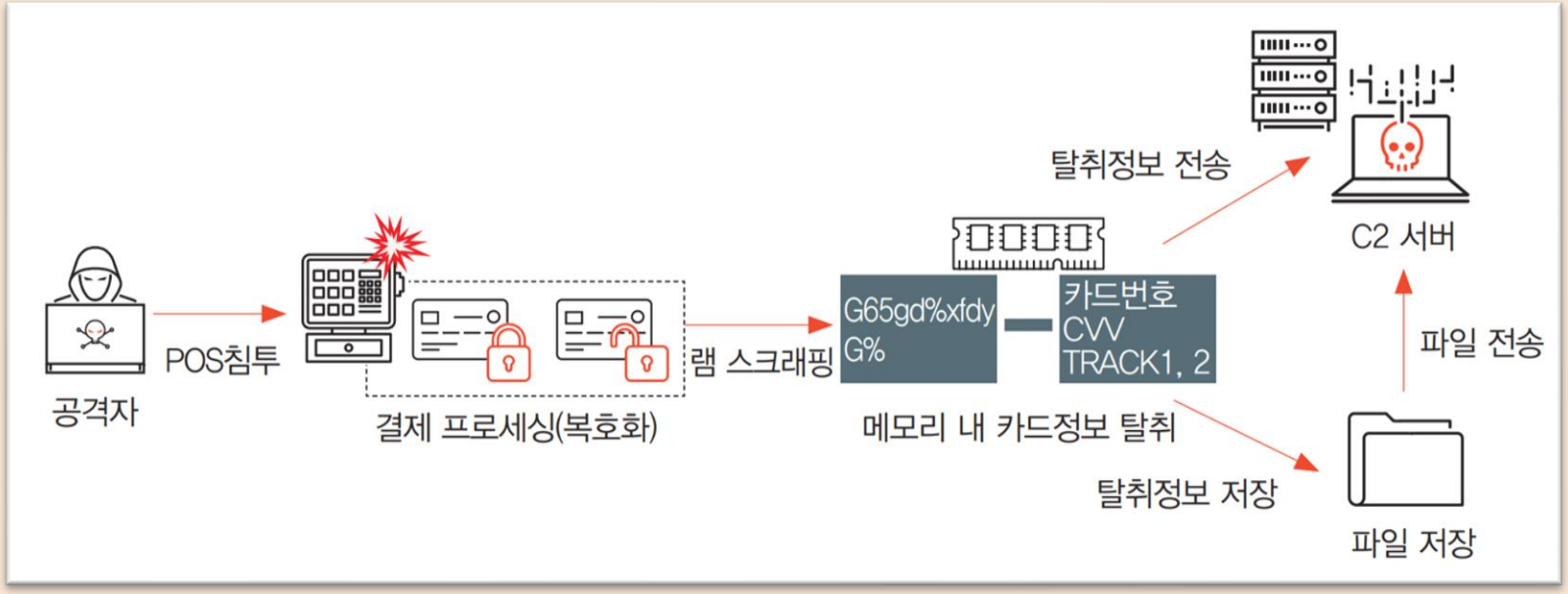
신용카드를 노리는 위협그룹 및 악성코드

POS 악성코드

- POS 악성코드의 핵심 기능은

  POS 관련 프로세스 내에 존재하는 카드결제 정보(이름, 카드번호, 만료 일자, CVC/CVV 등)를 탈취하는 것

- 카드결제 정보 탈취



신용카드를 노리는 위협그룹 및 악성코드

🖴 POS 악성코드 주요 기능

1) 초기 실행

- 주로 실행파일(exe) 형태로 유포되며, 정상 파일명으로 위장하는 방식으로 악성코드의 실행을 유도
- (초기) 단일 실행파일, 정상파일 위장, 자가복제
- (최근) VBA/파워쉘 등의 스크립트 형태, wmic(PUNCHTrack, BadHatch) 트리거, 서비스/스케줄 등록, 레지스트리 내 페이로드 저장

2) 정보 수집

- 램 스크래핑, 정류식, 룬알고리즘을 이용하여 카드 정보 수집
- (초기) Regex 기반 탐색, 전체 프로세스 리스트 탐색, 키로깅/브라우저 전송기능 후킹
- (최근) Custom Searching 알고리즘 기반 탐색, Blacklist 프로세스 탐색 제외, 키로깅/브라우저 크리덴셜 후킹

신용카드를 노리는 위협그룹 및 악성코드

🖴 POS 악성코드 주요 기능

3) 탐지 회피

- 파일리스, 인코딩, 암호화 등을 사용하며, 샌드박스 탐지 또는 분석도구 탐지 기법을 적용
- (초기) 윈도우 API 활용, 프로세스 인젝션
- (최근) 네이티브 API 활용, DLL/프로세스 인젝션, 파일리스 동작,
  AES, Triple-DES, RSA 등의 블록암호화, 비트연산 등을 활용한 인코딩 및 암호화, 커스텀 패킹

4) 정보 탈취

- 기본적인 파일 전송 프로토콜 뿐만 아니라 SMTP, DNS 터널링 기법을 사용하는 방식을 이용
- (초기) 탈취정보 평문 전송, Remote File Copy, FTP, SMTP, HTTP
- (최근) 탈취정보 인코딩/XOR 연산 후 전송, XTEA 경량암호화 적용 후 전송, HTTPS(불법 인증서)/HTTP, DNS 터널링

신용카드를 노리는 위협그룹 및 악성코드

POS 악성코드의 기능별 변화

- POS 악성코드는 지속적으로 진화 중
  → 보안 시스템의 탐지 및 차단을 회피
  → 탐지 및 추적이 어렵도록 탈취 정보 전송
  → 랜섬웨어와 혼합하여 공격 수행

- e-커머스 웹 사이트를 대상으로 한 E-skimming, Formjacking 기법을 활용한 카드 정보 탈취 급증
- 웹 사이트 내에 존재하는 자체 취약점 이용 또는 3rd party 서비스에 코드 삽입

구분	초기 POS 악성코드	최근 POS 악성코드
초기 실행	– 단일 실행파일 형태 – 정상파일 위장 – 자가복제	– VBA, 파워쉘 등의 스크립트 형태 – 난독화된 쉘코드 – WMIC 트리거 – 멀티 스테이지 실행 – 서비스, 스케쥴 등록 실행 – 레지스트리 내 페이로드 저장
정보 수집	– Regex 기반 탐색 – 전체 프로세스 리스트 탐색 – 키로깅, 브라우저 전송기능 후킹	– Custom Searching 알고리즘 기반 탐색 – Blacklist 프로세스 탐색 제외 – 키로깅, 브라우저 크리덴셜 후킹
탐지 회피	– 윈도우 API 활용 – 프로세스 인젝션	– 네이티브 API 활용 – DLL, 프로세스 인젝션 – 파일리스 동작 – AES, RSA 등 블록암호화 – XOR, ROR, ROL 등 비트연산 – API Hash 기반 함수 콜 – 커스텀 패킹, 코드 난독화
정보 탈취	– 탈취정보 평문 전송 – Remote File Copy – FTP / SMTP – HTTP	– 탈취정보 인코딩, XOR 연산 후 전송 – XTEA 경량암호화 적용 후 전송 – HTTPS(불법 인증서), HTTP – DNS 터널링

다크웹 암시장 현황 및 카드 정보 생명주기

다크웹 암시장 현황

- 다크웹은 익명성을 기반으로 동작하는 네트워크
- 초기의 다크웹은 개인의 이념과 사상을 탄압하는 국가에 대항하기 위한 정치적인 목적으로 이용
- 현재는 불법적인 마약, 불법 무기거래, 살인청부 등 불법적인 목적으로 이용(블랙마켓)

- 현재 다크웹에서 카드 정보가 거래되고 있는 블랙마켓의 형태는
  크게 '사이버 범죄 포럼', '마켓플레이스', '카딩샵' 총 3곳으로 분류 가능

다크웹 암시장 현황 및 카드 정보 생명주기

🖴 다크웹 암시장 현황

1) 사이버 범죄 포럼

- 서피스웹에서 운영되는 커뮤니티 포럼의 개념과 크게 다르지 않음
- 카드 정보를 사고팔거나 탈취된 정보들을 공개적으로 게시하는 등 포럼 내에서 암거래 시장을 형성
- 대표적인 곳 : RaidForum, Nulled, XSS Forum, Club2CRD 등

① 판매자가 판매 게시글을 올리고 구매자는 게시글 조회

② 구매자는 판매자가 남긴 사설 채널(텔레그램, Jabber, ICQ 등)로 구매의사 전달

③ 사설 채널을 통해 거래 진행

다크웹 암시장 현황 및 카드 정보 생명주기

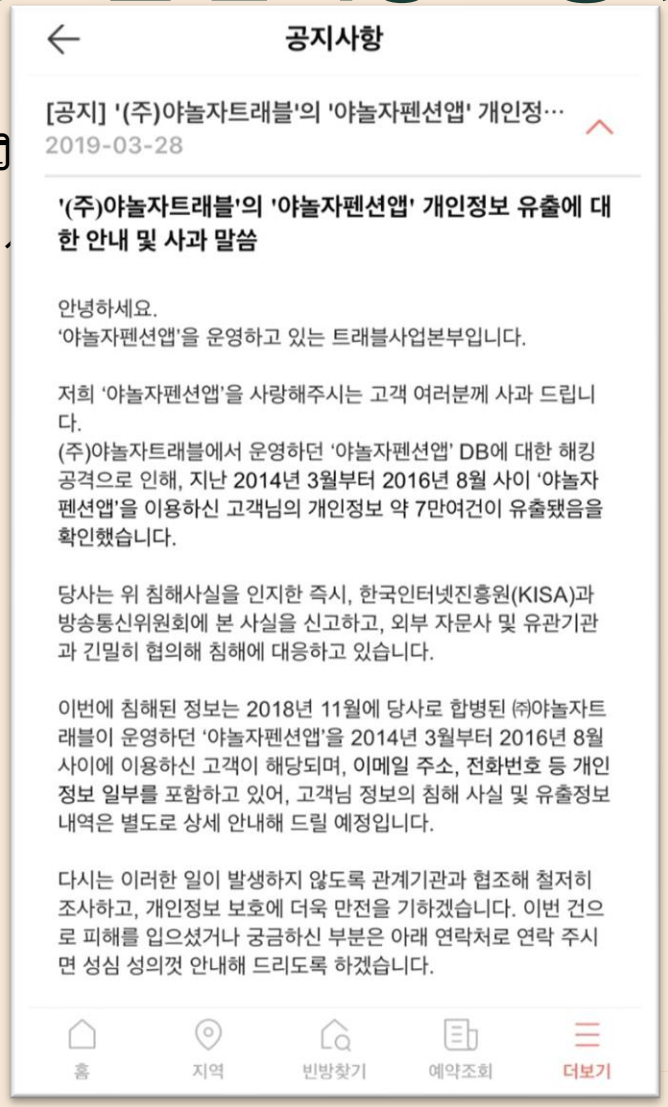
🖴 다크웹 암시장 현황

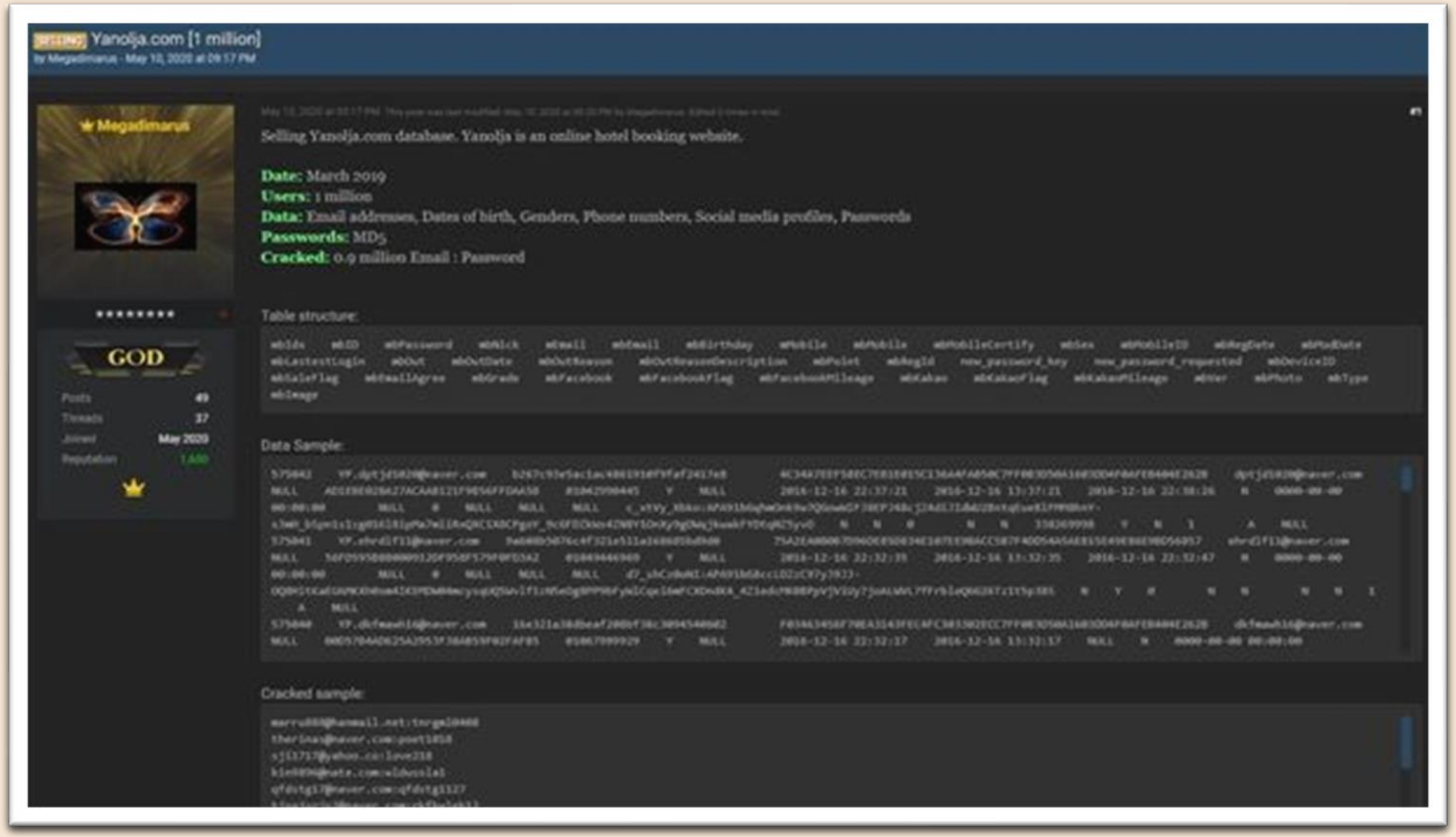
1) 사이버 범죄 포럼

- ex) RaidForum 사이트
  - 2015년 개설
  - 50만 명 이상의 회원 수
  - 게임 관련 접속 계정,
    해킹된 기업의 DB 덤프 등이
    공유되거나 거래됨
  - 해킹 툴에 대한 판매 및 방법에
    대한 공유도 이루어짐

다크웹 암시장 현황 및 카드 정보 생명주기

1)





다크웹 암시장 현황 및 카드 정보 생명주기

💳 다크웹 암시장 현황

2) 마켓플레이스

- 서피스웹에서 이용하는 인터넷 쇼핑몰을 생각하면 이해하기 쉬움
- 카드정보 외에도 마약, 총기, 모조품 등 다양한 카테고리의 상품들을 거래하는 곳
- 대표적인 곳 : DarkFox, WorldMarket, RussianMarket 등

① 판매자가 판매 게시글을 올리고 구매자는 게시글 조회

② 구매자는 상품 금액을 에스크로를 통해 입금

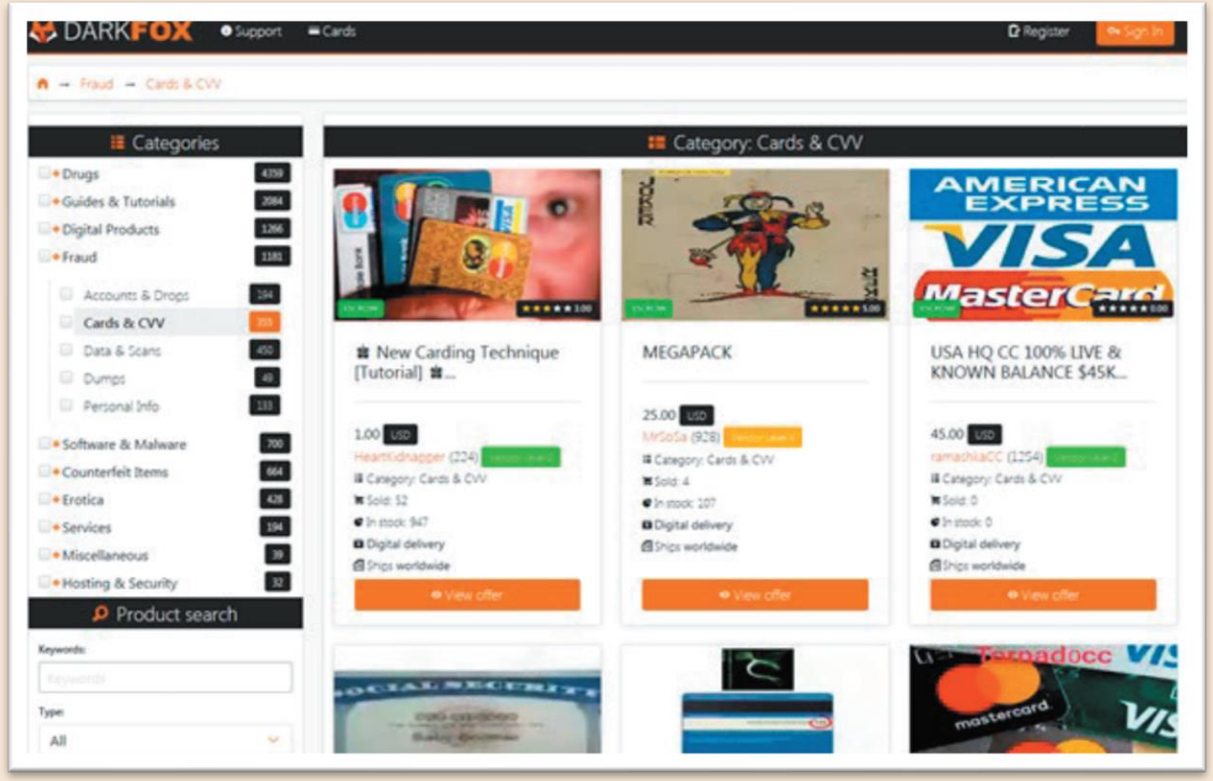
③ 판매자는 상품을 구매자에게 전달

다크웹 암시장 현황 및 카드 정보 생명주기

🖴 다크웹 암시장 현황

2) 마켓플레이스

- ex. DarkFox 사이트
  - 2020년 개설
  - 마약, 카드 정보, 악성코드, 모조품 등 판매
  - 판매자에 대한 등급제 시스템을 통해 구매자에게 신뢰성 보장
  - 안전한 거래를 위해 에스크로 서비스 지원



다크웹 암시장 현황 및 카드 정보 생명주기

💳 다크웹 암시장 현황

3) 카딩샵

- 다크웹 내에서 카드 정보만 전문적으로 취급하는 마켓플레이스
- 카딩샵의 경우에는 주로 1명의 벤더에 의해 운영되며 AVC(Automated Vending Carts) 형태로 운영
- 대표적인 곳 : Brian’s Club, Joker’s Stash, SwarmShop 등

① 운영자가 판매상품을 카딩샵에 등록

② 구매자는 자신의 계정에 금액을 충전하고 구매 상품을 조회

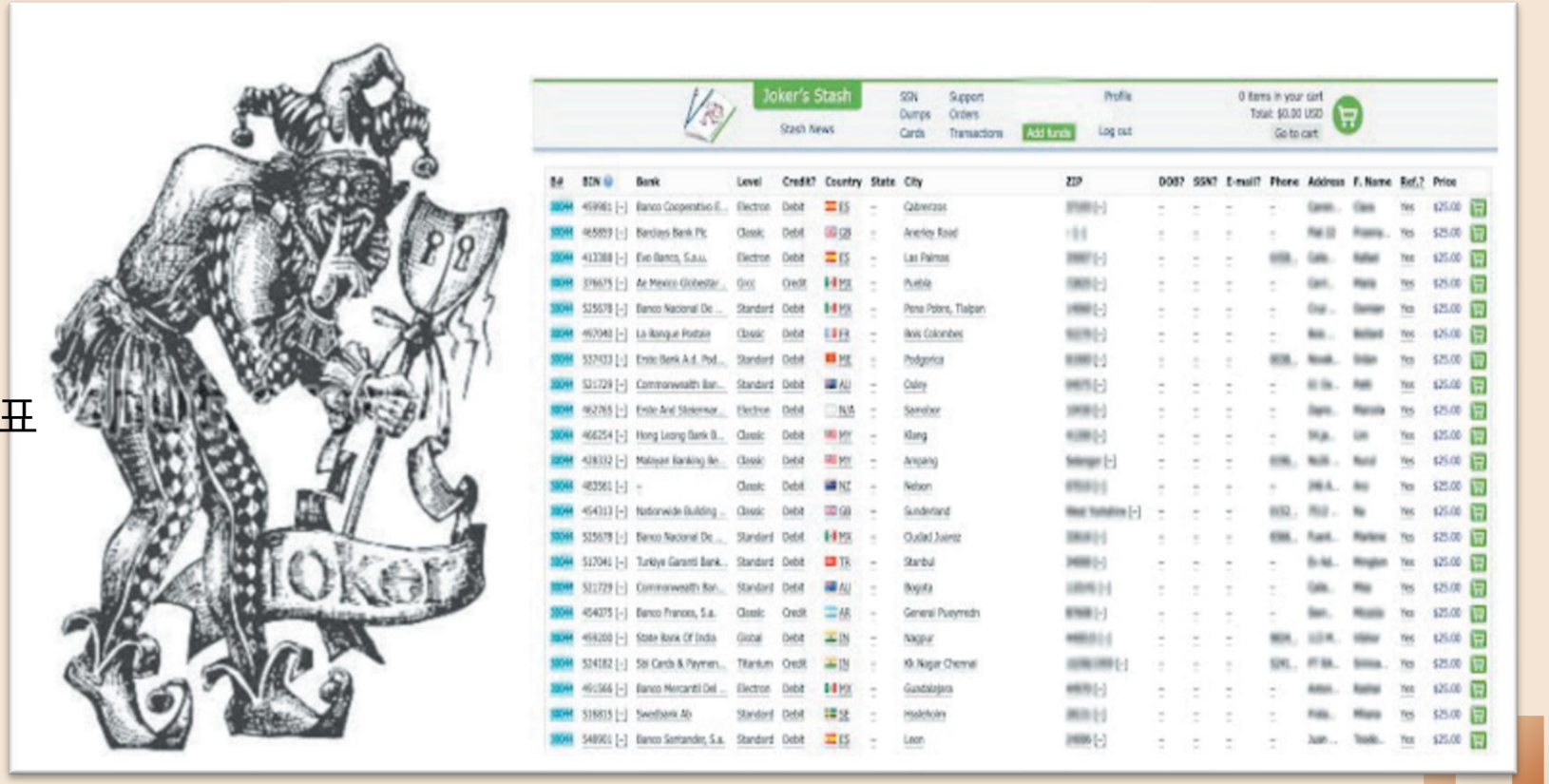
③ 구매자는 원하는 상품을 구매하고 자신의 계정 잔액에서 차감

다크웹 암시장 현황 및 카드 정보 생명주기

🖴 다크웹 암시장 현황

3) 카딩샵

- ex. Joker's Stash 카딩샵
  - 2014년 개설
  - 연간 10억 달러 이상의 비트코인을 번 것으로 추정
  - 2021년 2월 카딩샵 폐쇄 발표



다크웹 암시장 현황 및 카드 정보 생명주기

💳 카드 정보 생명주기

1) 유입

- 공격자가 카드 정보를 탈취하기 위해 POS 단말기 및 사용자PC에 악성코드를 설치하는 단계
- ⓐ사용자의 개입이나 ⓑ외부 공격, ⓒ취약한 업데이트 로직에 의해 악성코드가 유입됨

2) 결제

- 사용자가 신용카드를 이용하여 POS 단말기 등에서 결제하는 단계
- (오프라인) 주로 포스 단말기의 리더기를 통해 신용카드의 track2 정보 읽음

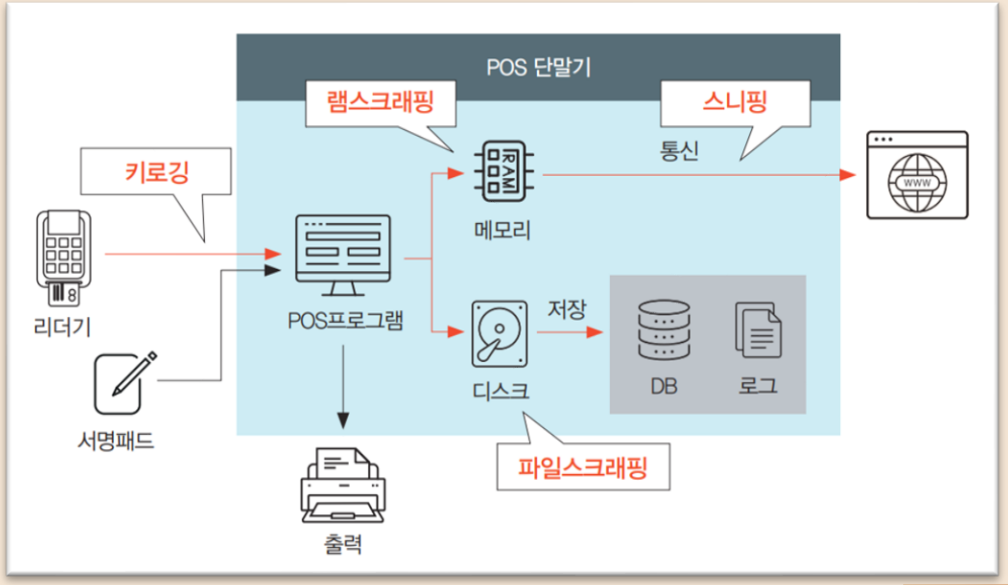
  → 프로그램 내에서 메모리, 디스크를 거쳐 외부로 통신 → 결제 진행
- (온라인) 카드번호, 유효기간, 보안코드를 입력 → 입력된 정보들 카드사로 전송 → 결제 프로세스 진행

다크웹 암시장 현황 및 카드 정보 생명주기

💳 카드 정보 생명주기

3) 탈취

- POS 단말기 등에 설치된 악성코드에 의해 카드 정보가 외부로 탈취 되는 단계
- 설치된 악성코드는 다양한 구간에서 신용카드 정보를 탈취함
  - 리더기에서 프로그램으로 전송되는 구간에서 키로깅
  - 결제 처리 과정에서 메모리/디스크/네트워크 통신 구간에서 데이터를 가로채기(램스크래핑, 파일스크래핑, 스니핑)



다크웹 암시장 현황 및 카드 정보 생명주기

💳 카드 정보 생명주기

4) 유통

- 탈취된 카드 정보를 판매, 복제카드를 이용하여 현금화, 유통되는 정보의 일부가 외부에 공개되는 단계
- (판매) 다크웹 암시장에 판매글을 올려 구매를 유도
- (유출) 다크웹에서 판매되는 카드정보가 또다른 공격자에게 유출되어 유료로 공개,
  또는 랜섬웨어 유포 그룹에서 협상을 유리하게 진행하기 위해 데이터 공개

5) 폐기

- 공개된 카드 정보를 FDS감시 또는 유효기간 만료로 인해 더 이상 악용이 불가능한 단계

감사합니다