금융미래를 열어가는 금융보안파트너

대한민국의 **안전한 금융환경**을 만들어가는 **금융보안원**

2019년 금융권 보안 위협 전망

FINANCIAL SECURITY
THREAT LANDSCAPE

금융보안원
FINANCIAL SECURITY INSTITUTE

대한민국의 안전한 금융을 만들어가는 금융보안원

2019년 금융권 보안 위협 전망

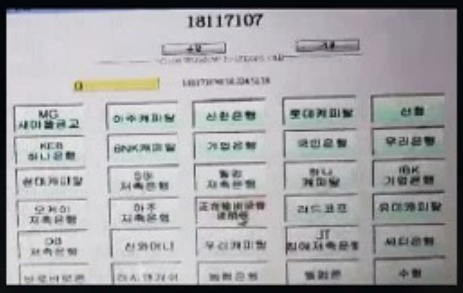
CONTENTS

금융보안원
FINANCIAL SECURITY INSTITUTE

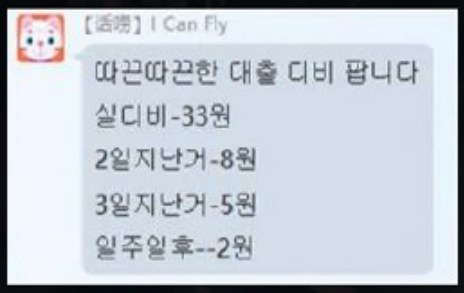
ISSUE **01.**

개인 금융정보가 거래되는 **블랙마켓** 확대

- **이미 판매된 관리자 계정 등이 변경된 경우 해당 웹사이트를 다시 해킹하여 변경된 계정정보를 알려주는 구매자 A/S 서비스도 존재**



[금융회사 사칭 ARS자동응답 프로그램]



[블랙마켓 개인정보 거래]

(씨엔시큐리티)

전망 및 대응방안

블랙마켓의 지속 성장 및 암호화폐 연계 거래 증가

- **금융권 사이버범죄는 즉각적인 금전적 이득을 취할 수 있어, 관련 정보를 쉽게 얻을 수 있는 블랙마켓도 계속 성장할 전망**
- **거래 시 익명성 보장을 위해 실제 화폐보다는 비트코인과 같은 암호화폐를 통한 거래가 증가할 것으로 예상**

  * 현재 공격자들은 블랙마켓 거래 시 위챗페이나 알리페이 등을 주로 이용

블랙마켓에 대한 지속적인 분석 및 예방 차원의 대응이 필요

- **블랙마켓에 쓰이는 은어(黑語, 헤이화)*를 이해하고, 정보 유통과정을 분석 하는 등 블랙마켓과 관련 현황을 적극 분석할 필요**

  * 블랙마켓에서는 SFZ(신분증), XYK(신용카드), W(만)와 같은 은어를 사용 중
- **웹사이트 계정에 대한 크리덴셜 스터핑 공격[3] 등 의심 행위 발생 시 이를 분석·차단하는 등 해킹사고 예방을 위한 대응활동에 만전을 기할 필요**

  ※ 고객DB를 이용하여 국내 금융권을 대상으로 로그인을 무작위로 시도하는 해킹공격 발생(`18.6월)
- **웹사이트 관리자 계정 정보 및 고객정보 등이 유출되지 않도록 단말기에 대한 보안은 물론 외부 유지보수 업체에 대한 보안관리도 중요**

3) 크리덴셜 스터핑(Credential Stuffing) : 공격자가 이미 확보한 계정과 비밀번호를 무차별 대입하여 로그인 후 사용자 정보를 추가로 유출하는 공격 기법

ISSUE **01.**

개인 금융정보가 거래되는 **블랙마켓** 확대

해킹 등을 통해 불법적으로 수집된 개인 금융정보 등이 인터넷상의 블랙마켓[1]을 통해 활발하게 거래되고 있으며 점차 확대 예상

보안위협 동향

❯ 블랙마켓에서 개인 금융정보 등 다양한 컨텐츠가 거래됨

- **공격자들은 금융사이트를 해킹하여 획득한 개인 금융정보나 금융 범죄에 악용될 수 있는 관리자(admin) 계정 또는 공격도구(웹쉘[2])을 블랙마켓에서 거래**

개인금융정보	금융 관련 사이트 계정, 대출관련 상담정보, 은행계좌 정보, 신용 카드 정보, 보안카드 및 OTP, 금융 거래 정보 등
금융범죄관련도구및서비스	웹사이트 관리자 권한, 금융사 사칭 ARS 프로그램, 웹쉘, 대포통장, 불법계좌 이체 의뢰, 웹사이트 해킹 대행 등

- **거래 금액은 수십만 원에서 수백만 원에 이르며, 구매자는 해당 정보를 광고, 대출 권유 등 금전적 이득을 위해 악용**

[블랙마켓의 웹사이트 관리자 계정 거래] (씨엔시큐리티)

❯ 금융 범죄를 위한 블랙마켓 거래 컨텐츠가 점차 진화

- **블랙마켓에서는 단순히 개인 금융정보만 거래되는 것이 아니라 국내 금융회사를 사칭하는 ARS 자동응답 프로그램 등 공격 툴도 판매**

1) 웹사이트 취약점, 개인정보, 관리자 권한 등 사이버범죄를 위한 정보 등이 불법적으로 거래되는 곳
2) 웹쉘(WebShell): 웹사이트의 업로드 취약점을 통해 시스템에 명령을 내릴 수 있는 코드를 의미하며, 공격자는 웹쉘을 통해 별도의 인증 없이 시스템에 쉽게 접속하여 명령을 내릴 수 있음