将来の金融を開いていく金融セキュリティのパートナー

대한민국의 **안전한 금융환경**을 만들어가는 **금융보안원**

2019年、金融界のセキュリティ脅威の展望

FINANCIAL SECURITY
THREAT LANDSCAPE

금융보안원 金融保安院

CONTENTS

ISSUE 01.
個人の金融情報が取引されているブラックマーケットの拡大

ISSUE 02.
클라우드, 사물인터넷 등 IT **新기술 악용 공격** 증가

ISSUE 03.
Mac OS 악성코드 증가로 인한 오픈뱅킹 위협

ISSUE 04.
점점 더 교묘히 **암호화폐**를 채굴해가는 공격자들

ISSUE 05.
해킹그룹의 정교한 금융권 내부 **APT 공격** 확대

ISSUE 06.
보이스피싱 진화 등 지능화된 **모바일 보안** 위협

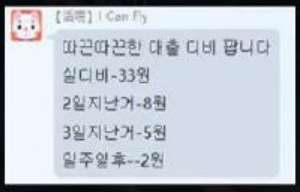
ISSUE 07.
ATM, SWIFT 등 **지급결제시스템 공격** 확대

ISSUE **01.**

個人の金融情報が取引されているブラックマーケットの拡大

- 既に販売されていた管理者のアカウントなどが変更された場合、そのウェブサイトを再度ハッキングして変更されたアカウント情報を知らせる買い手のためのA/Sサービスも存在

金融会社を詐称するARS知能応答プログラム



ブラックマーケットの個人情報の取引

「シエンセキュリティ」

展望と対応策

ブラックマーケットの持続的な成長と仮想通貨の連携取引が増加

- 金融圏のサイバー犯罪は、即刻的な金銭的利益を上げることができ、関連情報を簡単に得ることができるブラックマーケットも引き続き成長する見通し
- 取引時の匿名性を保証するために、実際の貨幣ではなく、ビットコインのような仮想通貨を通じた取引増加すると予想
  - 現在、攻撃者たちはブラックマーケット取引の際、ウィチェッペイやアリペイなどを主に利用

ブラックマーケットの継続的な分析と予防の対応が必要

- ブラックマーケットで使われる隠語(黒话、ヘイファ)を理解して、情報流通の過程を分析するなどブラックマーケットと関連の現況を積極的に分析することが必要
  - ブラックマーケットでは、SFZ(身分証)、XYK)クレジットカード)、W(万)のような隠語を使用中
- ウェブサイトのアカウントに対したクレデンシャルスタッフィング攻撃などの疑惑行為が発生する時に、これを分析、遮断するなどのハッキング事故の予防に向けた対応活動が必要
  - ※ 顧客のDBを利用して、国内の金融圏を対象にログインをランダムにしようとするハッキング攻撃発生('18.06)
- ウェブサイトの管理者のアカウント情報や顧客情報などが流出しないように端末機のセキュリティはもちろん、外部のメンテナンス会社のセキュリティ管理も重要

クレデンシャルスタッフィング(Credential Stuffing) ：攻撃者がすでに確保したアカウントとパスワードをブルートフォースしてログインした後、ユーザーの情報を追加で流出する攻撃手法

ISSUE **01.**

個人の金融情報が取引されているブラックマーケットの拡大

ハッキングなどを通じて違法に収集された個人の金融情報などがインターネット上のブラックマーケットを通じて活発に取引されており、徐々に拡大予想

セキュリティ脅威の動向

ブラックマーケットで個人の金融情報など、様々なコンテンツが取引される

- 攻撃者たちは金融サイトをハッキングして獲得した個人金融情報や金融犯罪に悪用されることができる管理者(admin)のアカウントまたは攻撃ツール(Webshell)をブラックマーケットでの取引

個人の金融情報	金融関連サイトのアカウント、ローン関連の相談の情報、銀行口座の情報、クレジットカードの情報、セキュリティカードとOTP、金融取引の情報など
金融犯罪関連ツールとサービス	ウェブサイトの管理者の権限、金融機関の詐称のARSプログラム、Webshell、大砲通帳、不法口座振替依頼、Webサイトのハッキング代行など

- 取引金額は数十万ウォンから数百万ウォンに達し、買い手はその情報を広告、融資の勧誘など金銭的な利益のために悪用

ブラックマーケットのウェブサイトの管理者のアカウント取引(シーエヌセキュリティ)

金融犯罪のためのブラックマーケット取引のコンテンツが徐々に進化

- ブラックマーケットでは、単に個人の金融情報のみ取引されるのではなく、国内の金融会社を詐称するARSの自動応答プログラムなどの攻撃ツールも販売