Semkel

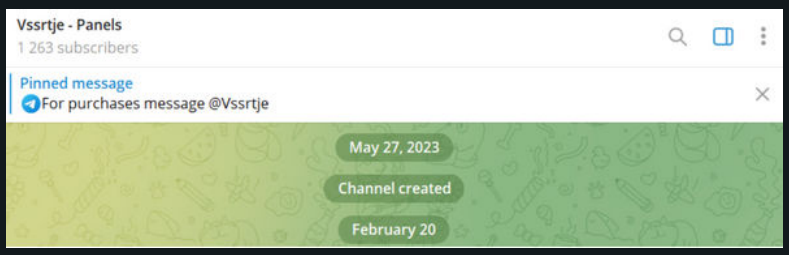
Kit Phishing x Banque

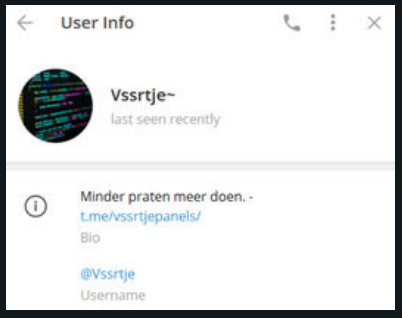
06/2024

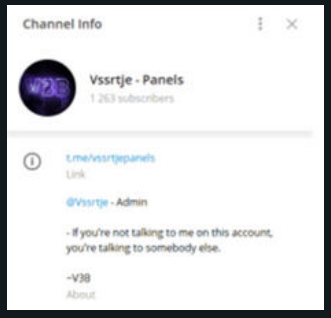
SEMKEL.COM

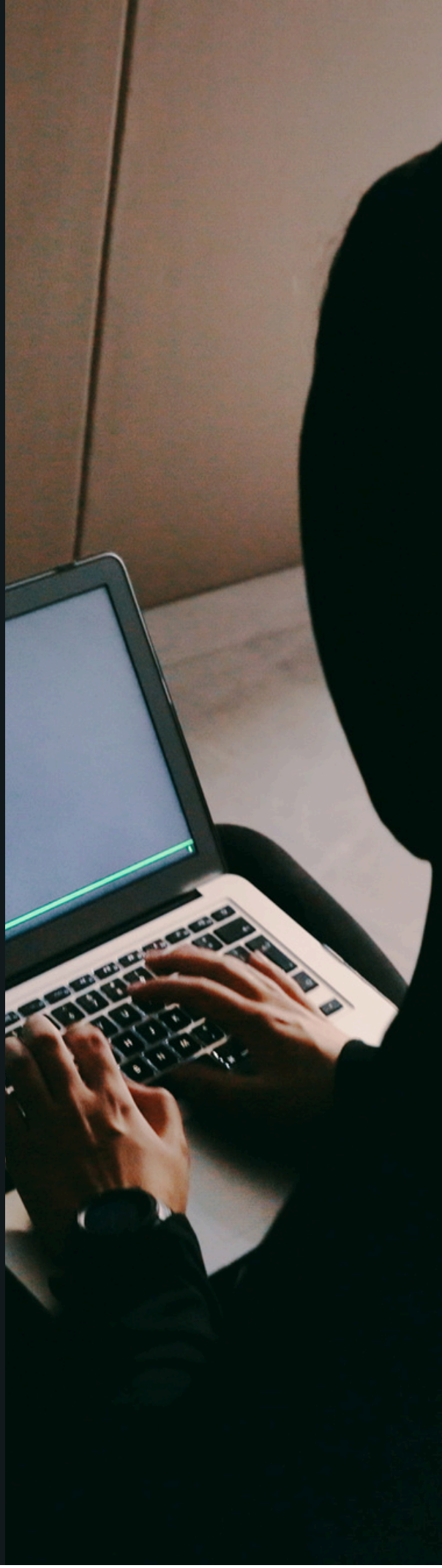
Un nouvel acteur de la menace Vssrtje commercialise un kit de phishing menaçant les banques européennes et françaises

Un nouvel acteur de la menace, le groupe Vssrtje, propose des kits de phishing sophistiqués aux fraudeurs ciblant les clients bancaires de l'UE. Ces kits interceptent des informations sensibles, telles que les identifiants et les codes SMS/OTP (One Time Password), en utilisant des techniques d'ingénierie sociale. Distribué sous le modèle Phishing-as-a-Service (PhaaS) et en auto-hébergement, le kit "V3B" est promu sur la chaine Telegram @vssrtjepanels, administré par @Vssrtje et crée le 27 mai 2023 mais active depuis le 20 février (Il est possible que les messages précédents aient été supprimés). Cette chaîne Telegram compte plus de 1263 membres en date du 11 juin 2024, ce qui témoigne de l'ampleur de leurs activités. Des centaines de cybercriminels ont adopté le kit V3B, laissant les victimes avec des comptes bancaires vides.









PROFIL DES MEMBRES

La majorité des membres de cette chaîne sont des cybercriminels spécialisés dans diverses formes de fraude, telles que l'ingénierie sociale, l'échange de cartes SIM, la fraude bancaire et de cartes de crédit. Pour l'heure il n'est pas possible d'identifier formellement les pays depuis lesquels ils agissent.

Ces acteurs malveillants ciblent principalement les banques de l'UE, dont la France, entraînant des pertes financières importantes pour les clients bancaires européens, estimées à plusieurs millions d'euros.

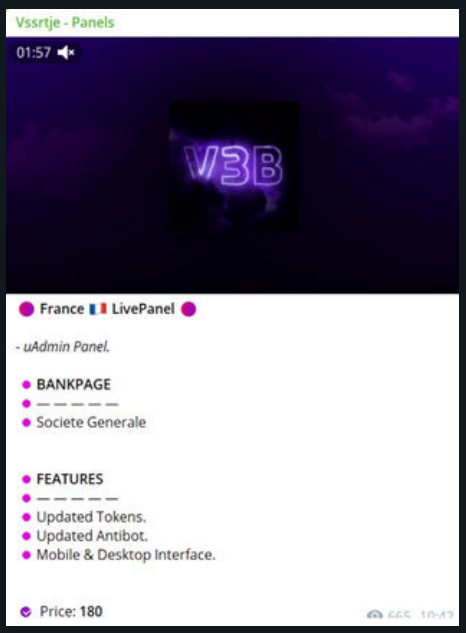
Avec l'augmentation de ces attaques contre les institutions bancaires, on peut observer en parallèle la croissance des réseaux de mules financières en Europe. Les mules financières jouent un rôle crucial dans le blanchiment d'argent et le transfert de fonds volés, rendant plus difficile la traçabilité et l'identification des auteurs des crimes.

TYPOLOGIE DES VICTIMES

Les victimes de ces kits de phishing, chacun personnalisé pour cibler des banques spécifiques, sont clients de 54 institutions bancaires dont les banques françaises suivantes :

- Caisse d'Épargne
- Banque Populaire
- Boursorama Banque
- Société Générale
- HSBC
- Hello Bank
- BNP Paribas
- ING Bank
- AXA Bank
- Crédit Agricole

PRIX ET CARACTÉRISTIQUES



Le prix du kit de phishing varie de 80 $ à 450 $ par mois, payable en crypto-monnaie. Le coût dépend des modules spécifiques et des banques prises en charge. L'auteur du kit publie régulièrement des mises à jour et ajoute de nouvelles fonctionnalités pour échapper à la détection, telles que des algorithmes de vol d'informations d'identifications améliorés et des techniques d'obscurcissement avancées.

MODE OPÉRATOIRE

Le kit de phishing V3B prend en charge plus de 54 institutions financières en offrant des modèles personnalisés et localisés. Ces modèles imitent les processus d'authentification et de vérification des systèmes bancaires en ligne et de commerce électronique dans toute l'UE, garantissant une apparence réaliste et adaptée à chaque institution ciblée.

Le code des kits de phishing est crypté et obscurci via JavaScript pour échapper à la détection par les systèmes anti-phishing et les moteurs de recherche, protégeant ainsi ses codes sources de l'analyse des signatures.

Il inclut des fonctionnalités avancées telles que des jetons mis à jour, des mesures anti-bot, des interfaces mobiles et de bureau, un chat en direct avec les victimes, et la prise en charge des OTP/TAN/2FA, y compris les codes QR et la méthode PhotoTAN.

Construit sur un CMS personnalisé avec des scénarios obscurcis, le kit assure une persistance prolongée en ligne en échappant à la détection.

FONCTIONNALITÉS

L’uPanel permet aux fraudeurs d’initier une demande OTP ou jeton, incitant les victimes à saisir leurs codes, que les fraudeurs utilisent ensuite pour vérifier les transactions. Le kit utilise l’API Telegram comme canal de communication pour transmettre les données de paiement interceptées au fraudeur, l’alertant de la réussite de l’attaque.
Un système anti-bot avancé détecte et empêche la détection par les bots, les robots et les outils de sécurité. Le kit offre des capacités de localisation avancées avec des pages traduites en plusieurs langues, notamment le finnois, le français, l’italien, le polonais et l’allemand.

Le kit de phishing intègre un système avancé permettant aux fraudeurs d’interagir en temps réel avec les victimes. Par exemple, un acteur peut inciter une victime à saisir un code PushTAN et déclencher une demande OTP par SMS pour le collecter, contournant ainsi la validation OTP. Lorsqu'une victime accède à la page d’hameçonnage, le fraudeur est immédiatement informé via un «avertissement» proactif, lui permettant de déclencher des actions spécifiques.

Les différentes combinaisons de déclencheurs permettent une interaction directe et en temps réel avec la victime, donnant au kit de phishing la capacité de mener des actions spécifiques. Cela facilite l'accès illégal aux comptes et permet d'exécuter des transactions frauduleuses.

ÉVÈNEMENTS DECLENCHÉS PAR LE KIT

Le kit de phishing déclenche une série d'événements, tels que des demandes de connexion, de SMS/OTP, d’informations de carte de crédit, de numéros de téléphone, d’adresses e-mail et de dates de naissance. Il inclut également des demandes de PhotoTAN, de SmartID et de codes QR, ainsi que l'affichage de notifications personnalisées et de données provenant d'applications MFA.

Ce vaste éventail d'événements permet de cibler un grand nombre de banques. En utilisant des techniques avancées, le kit parvient à contourner la plupart des mesures de sécurité actuelles, rendant la protection traditionnelle inefficace contre ces attaques sophistiquées. Les fraudeurs peuvent ainsi exploiter l'accès compromis pour collecter des informations sensibles de manière efficace.

Le kit est conçu pour être extrêmement adaptable et peut être configuré pour répondre à des exigences spécifiques, maximisant ainsi son efficacité et sa portée dans les campagnes de phishing. Cette flexibilité permet de maintenir une longueur d'avance sur les nouvelles mesures de sécurité mises en place par les institutions financières, garantissant que les attaques restent efficaces même face à des systèmes de défense de plus en plus sophistiqués.

ANALYSE ET PERSPECTIVE AVEC L’ARRIVÉE DE NIS2

L'Union européenne, avec son économie développée et son système financier mature, est particulièrement vulnérable, avec des pertes estimées à des centaines de millions d’euros dues à la cybercriminalité et à la fraude financière. La cybercriminalité est une menace économique mondiale majeure, avec des pertes estimées à 11,50 billions de dollars en 2023. Les prévisions du FBI, du FMI et d'autres organisations indiquent que la cybercriminalité pourrait atteindre 23 billions de dollars d'ici 2027, représentant une préoccupation croissante pour les organisations de toutes tailles.

Les kits de phishing comme V3B, disponibles sur le Dark Web, contribuent à ces pertes importantes. Facilement accessibles et abordables, ces outils permettent aux fraudeurs de causer des pertes financières massives.

Pour prévenir efficacement la fraude, les banques doivent adopter une approche proactive en collectant des renseignements sur le Dark Web, se tenant informées des outils tels que V3B, et en mettant continuellement à jour leurs stratégies et contrôles de sécurité. Cela implique de surveiller le Dark Web pour identifier les nouveaux outils et techniques utilisés par les cybercriminels, ainsi que d'améliorer les processus d'authentification et de vérification pour prévenir les activités frauduleuses.

La directive NIS2 (Network and Information Systems Directive 2), adoptée par l'Union européenne, vise à renforcer la cybersécurité des infrastructures critiques, y compris le secteur bancaire. En réponse à l'augmentation des cybermenaces, NIS2 impose des obligations plus strictes aux entités essentielles, notamment les banques, pour améliorer leur résilience face aux cyberattaques. Les mesures préventives décrites ci-dessus sont en ligne avec les exigences de la directive NIS2.

En particulier, la surveillance proactive et le partage d'informations répondent aux exigences de NIS2 en matière de surveillance continue des menaces et de collaboration accrue entre les entités pour partager des renseignements sur les cybermenaces.

La collecte de renseignements sur le Dark Web et la mise à jour des stratégies de sécurité bancaire permettent aux institutions de se préparer et de répondre rapidement aux nouvelles menaces comme les kits de phishing V3B.

En intégrant ces mesures, les banques peuvent non seulement se conformer à la directive NIS2 mais aussi réduire significativement leur exposition aux risques cybernétiques, contribuant ainsi à la protection de l'ensemble du système financier de l'UE.

Semkel est une société de services et de conseil en Risk and Threat Intelligence dédiée à la protection des intérêts économiques et numériques de ses clients à travers des services d'enquêtes et de surveillance.

SEMKEL.COM

Semkel SA, société anonyme à conseil d'administration au capital de
2 702 000€. 37 rue Dumois-Crancé 69600 Oullins.
R.C.S. Lyon 894 689 975 – SIRET : 89468997500015 – APE : 6312Z a