Mphasis
The Next Applied

V3B Phishing-as-a-Service (PhaaS) Platform

Date: 7th June 2024 | Severity: High

Summary

The V3B phishing-as-a-service (PhaaS) platform, first reported by cybersecurity researchers in June 2024, has been active since at least March 2023. The PhaaS primarily targets the customers of financial institutions in European countries.

Attack Vectors

V3B enables its subscribers to carry out various types of fraudulent operations, including social engineering, SIM swapping, and credit card theft. The phishing kit includes two primary components: a scenario-based credential interception system (V3B) and templates to mimic online banking authorization pages. To evade detection, the phishing pages are obfuscated with JavaScript code on top of a custom CMS. V3B also has an admin panel (uPanel) that enables fraudsters to conduct live chats with their victims and obtain one-time passwords (OTP) by sending them custom notifications. In addition, the platform also enables users to generate QR codes for phishing pages and supports PhotoTAN and Smart ID to bypass advanced authentication mechanisms. The stolen victim information is sent to the threat actors through the Telegram API.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• verifieer-gegevens{.}com • ics-cards{.}org • kundenaktualisierungen{.}cc • icscards-nl{.}com
File Hash	• 20e77ddc3fe017e1bd711317adc86494 • 3151764ce732dae8b863e15042ec2ac3 • 9589194ff77c2edb9a2e89765f570c5e • 00a1b728410ef6fee05fff9bde46e541

URLs	• http{:}//verifieer-nu{.}com/verificatie/66422f472f10c
	• http{:}//kontoaktualisierer-nl{.}com/icscard{.}nl-v1
	• http{:}//lcs-valideren{.}online/ics/sca-app/663e0152c96c0

	• http{:}//ics-beveiligde-verificatie{.}com/sqi{.}php
	• http{:}//bvstigveriapp{.}online/pay/664130fb17583
	• http{:}//reaktivieren-icsservice{.}nl/icscard{.}nl-v1/ics-log{.}php
	• http{:}//reaktivieren-icsservice{.}nl/icscard{.}nl-v1/
	• http{:}//valideren-mijn-ics-web1{.}online/sq0{.}php?session=664483b236193
	• http{:}//bunq-app-nl{.}net/K8IjL9/1M3k/lgn
	• http{:}//app-lnloggen{.}online/authenticatie/inloggen/nl
	• http{:}//abnamro{.}nl-appverifi{.}com/3/jjfosp/o34432fpo/index4{.}php
	• http{:}//gemiste-aanmaning{.}com/belasting
	• http{:}//redirect-bunq-client{.}ru/account/321/
	• https{:}//mijni- cs{.}bezoeknummer0734859938{.}info/sca/7a970ca144c3e89685550829fe62941/login

Recommendation

- Employee Training and Awareness: Regularly train employees on how to identify phishing attempts.
- Implement Multi-Factor Authentication (MFA): Require employees to use multi-factor authentication for accessing sensitive systems and data.
- Email Filtering and Spam Detection: Deploy robust email filtering and spam detection mechanisms to automatically identify and quarantine phishing emails before they reach employees' inboxes.
- Security Software and Firewalls: Utilize up-to-date security software and firewalls to detect and block phishing attempts, malware, and other malicious activities.
- Incident Response Plan: Develop and regularly update an incident response plans.
- Continuous Monitoring and Threat Intelligence.
- Penetration Testing and Security Audits: Conduct regular penetration testing and security audits to identify vulnerabilities in your systems and processes that could be exploited by phishing attacks.
- Legal and Law Enforcement Collaboration: Work closely with legal counsel and law enforcement agencies to investigate and prosecute individuals or groups behind phishing-as-a-service platforms like V3B.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://dashboard.ti.insight.rapid7.com/#/tip/cyberterm/6661cb0711497327889610d3
- https://www.resecurity.com/blog/article/cybercriminals-attack-banking-customers-in-eu-with-v3b-phishing-

Copyright © Mphasis Corporation. All rights reserved