Custom-Built Phishing Pages Include ID Upload and Selfie Cam

From Insikt Group

October 4, 2022

This report details pre-built and custom-built phishing pages offered by threat actors that include additional functionality beyond the typical functions. The target audience of this report is law enforcement and cyber threat intelligence (CTI) and fraud teams at financial institutions and card networks.

Executive Summary

Phishing schemes are becoming increasingly sophisticated and are constantly evolving to include new ways to win over a potential victim. Phishing pages targeting financial institutions have historically included functionality for collecting bank account login credentials, bank account information, payment card data, additional personally identifiable information (PII), and browser fingerprints. As threat actors continue to improve their methods, we have observed phishing pages with additional functionality designed to increase victim's "trust" in the phishing pages and to increase threat actors' capacity to pivot to second-stage fraud schemes.

In one example, we observed a threat actor who offered customized solutions for phishing pages that included features for identification (ID) document uploads and selfie camera verification. These features — combined with the typical data collected through phishing pages — would increase threat actors' ability to bypass identity verification checks that require ID documents or facial images, such as during fraudulent loan applications.

Key Judgments

- The threat actor "KNYGHT" offers custom-built phishing pages with a wide range of functionality, including the capability to request ID documents and a selfie to "confirm identity". KNYGHT offers the phishing pages on the "Exploitforum" page of the blog-hosting platform Blogger.
- KNYGHT's phishing pages collect bank account login credentials, bank account information, payment card data, additional PII, and browser fingerprints, as well as email address login credentials, ID documents, and selfies.
- Dark web threat actors try to make the phishing page look as real as possible by implementing various tools that are familiar to users, such as Google's CAPTCHA, input validation, or page adaptability, depending on the device used by the victim.

Background

Phishing is a type of social engineering in which cybercriminals send a fraudulent message designed to trick a victim into revealing sensitive information such as PII and bank information, or to deploy malicious software on the target infrastructure. The information stolen during phishing may then be directly used by scammers or sold to other cybercriminals to carry out various fraudulent activities. Over the past several years, phishing attacks have become increasingly more sophisticated, with threat actors finding more creative ways to steal personal data that can then be used fraudulently. As of 2021, according to the FBI's Internet Crime Complaint Center, phishing is by far the most common kind of attack performed by cybercriminals.

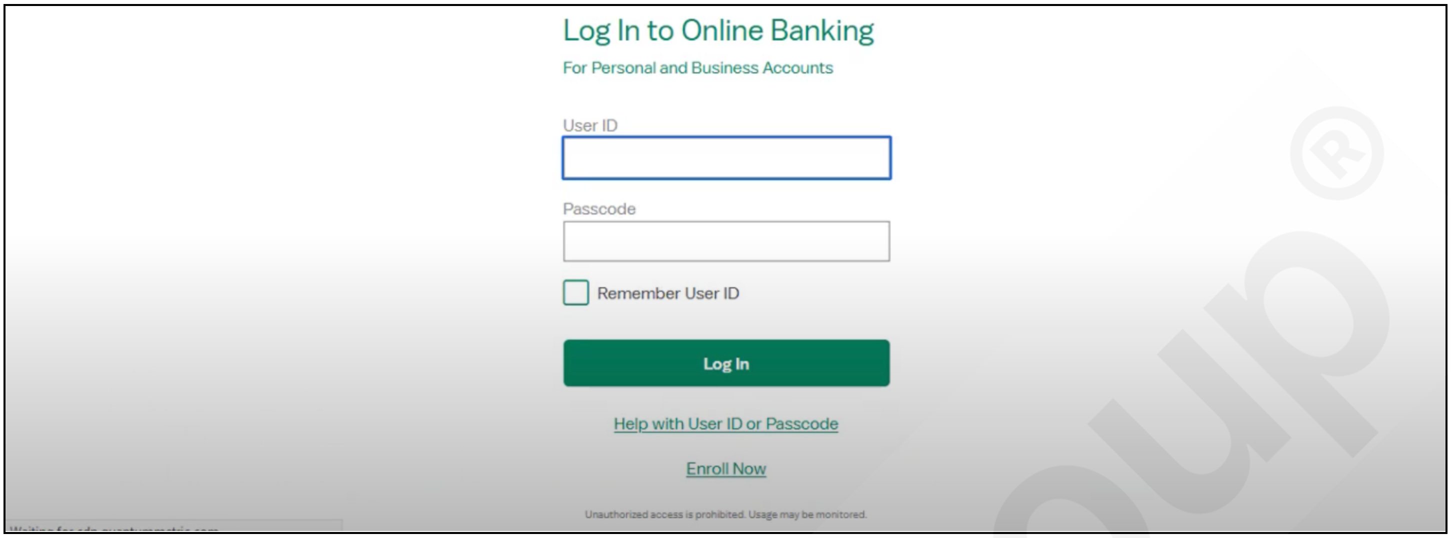
Threat Analysis

The threat actor "KNYGHT" offers custom-built phishing pages with a wide range of functionality, including the capability to request ID documents and a selfie to "confirm identity". The complete set of data that a threat actor could obtain through a phishing page of this type — bank account login credentials, bank account information, payment card data, additional PII, browser fingerprints, ID documents, and a selfie — would greatly increase the capacity of threat actors to conduct a wide range of fraudulent activity.

KNYGHT advertised the custom-built phishing pages on the "Exploitforum" page of the blog-hosting platform Blogger, alongside advertisements for pre-built phishing pages for various large banking institutions. In the advertisement, the threat actor listed the functionality of the bank's phishing pages and posted a video showing how the full phishing panel works.

How the Phishing Panel Works

Recorded Future sources contacted the threat actor KNYGHT and initiated a correspondence to gather additional details about the phishing panel. The sections below synthesize information from the advertisement, video, and correspondence with KNYGHT to reveal the phishing panel's features.



Log In to Online Banking

For Personal and Business Accounts

User ID

Passcode

□ Remember User ID

Help with User ID or Passcode

Enroll Now

Unauthorized access is prohibited. Usage may be monitored.

Figure 1: *KNYGHT advertising phishing page (Source: KNYGHT)*

Cybercriminal Buyers Responsible for Hosting the Phishing Page and Attracting Victims

According to the information provided by the threat actor in the video, once fraudulent actors purchase a template of the phishing page, they can employ it by assigning it to any domain and hosting under their control. Any successfully stolen data is sent to a data archive on the fraudulent actor's domain and also to their Telegram account or email address.

According to the threat actor, each fraudulent actor using the phishing page template is responsible for attracting potential victims to their phishing domain. In general, fraudulent actors use various means to attract victims including mass phishing campaigns via spam emails and semi-targeted campaigns via search engines and advertising on social networks.

Phishing Account Information, Payment Card Data, PII, and Browser Fingerprint

The video posted in KNYGHT's advertisement shows the functionality of their phishing page. In the video, after online bank login credentials are entered, the user is forced to perform "Account Verification", which gathers additional information from the victim. In the video, the phishing page appears to contain the following fields:

- Name and address information
- Payment card data (card number, expiration date, card verification value [CVV], and PIN number)
- Additional PII (email address, phone number, date of birth, and Social Security number [SSN])

Modern tools allow cybercriminals to easily customize the available fields on a phishing page based on buyers' requests. In correspondence with the Recorded Future source, KNYGHT indicated that they would customize the phishing page upon request.

As is typical for phishing pages, the page of the banking institution offered by KNYGHT also collects victims' browser fingerprint, which includes the victim's IP address and User Agent data (browser type and version, language, and operating system). The victim's browser fingerprint is important for fraudulent actors because it allows them to impersonate the victim more effectively and bypass anti-fraud detection when attempting to monetize a compromised bank account and/or payment card.

As a rule, financial institutions use anti-fraud measures to check that a transaction is made from a location and/or with a device that matches typical customer behavior. However, fraudulent actors can simulate a victim's system and geodata during a fraudulent transaction by leveraging a victim's browser fingerprint through the use of anti-detect browsers and SOCKS proxies, thereby greatly increasing their chances of success.

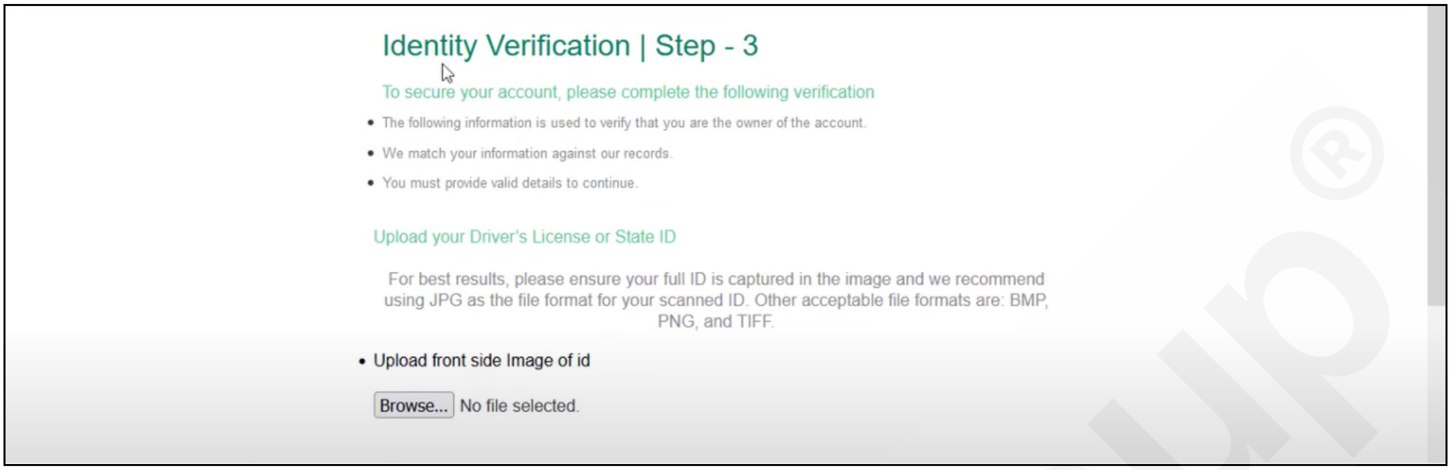
Phishing Email Account Login Credentials

The video also reveals that the bank phishing page contains a stage purportedly for verifying an email address for secure transactions. In this stage, a fictitious webpage is displayed, offering several common email providers. Once the victim chooses their provider, they are directed to another phishing page that mimics the chosen email provider, resulting in the exposure of inputted email login credentials. Upon entering the email login credentials, the victim is "redirected" back to the fraudulent Account Verification page, where they are alerted that the verification was "successful". Upon completion of this final stage, the victim is then directed to the legitimate bank login page.

Advanced Phishing Options for ID Documents and Selfies

In correspondence with Recorded Future sources, KNYGHT claimed that they are currently implementing 2 new features for the bank phishing page: ID document upload and a "selfie cam" for identity verification. The ID document upload feature would require victims to upload images of their driver's license and/or passport. Images of these documents are highly valuable to fraudulent actors as they could be used for obtaining fraudulent loans.

The "selfie cam" for identity verification would require the victim to take a selfie while holding an ID, as the site captures the victim's computer camera feed in real time. With various types of websites now turning to image and video identity verification, fraudulent actors would be able to reuse images stolen through this feature to bypass legitimate identity verification checks, which could enable them to conduct an even wider range of fraud activity.



Identity Verification | Step - 3

To secure your account, please complete the following verification

- The following information is used to verify that you are the owner of the account.
- We match your information against our records.
- You must provide valid details to continue.

Upload your Driver's License or State ID

For best results, please ensure your full ID is captured in the image and we recommend using JPG as the file format for your scanned ID. Other acceptable file formats are: BMP, PNG, and TIFF.

- Upload front side Image of id

Browse... No file selected.

Figure 2: *The phishing page requesting ID document upload and a "selfie cam" for identity verification (Source: KNYGHT)*

Backend Features for Higher "Legitimacy"

To instill more confidence in the user, the phishing page prompts the user to perform a CAPTCHA challenge-response test. The CAPTCHA is also used to protect the phishing page against bots such as crawlers. Moreover, the phishing page includes input validation, which checks to ensure that legitimate values are inputted for given fields (for example, that payment card number fields include digits). The victim is only able to proceed to the next stage of the fake "Account Verification" if fields contain "valid" data. Additionally, the phishing page can detect the user's device — such as a mobile phone or computer — and automatically adapt the webpage to it.

Mitigations

- Educate customers and explain the key items to watch out for.
- Deploy a spam filter used to detect indicators of phishing such as viruses, blank senders, and keyword text triggers.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a password security policy that includes but is not limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- For enterprises, Recorded Future can monitor for potential typosquat domains weaponized in phishing attacks. This includes not only the domains belonging to one's organization, but also third-party partners and vendors with enterprise network access.

Using the Recorded Future® Platform, clients can identify phishing and spamming widely used by threat actors to target their brand, which may indicate planned phishing or spamming attacks against them. Setting up Platform alerts allows a user to monitor for phishing updates and tactics, techniques, and procedures (TTPs) being used by threat actors.

Outlook

Recorded Future analysts did not use the phishing pages advertised by KNYGHT, as this would require the theft of personal and banking data. However, the components of the phishing panels — ready-to-use phishing pages, an archive of data inputted on the phishing pages, and the option to launch modules or pages while the victim's browsing session is active (for example, to send the fake 3DS verification pages) — are technically simple. This indicates that it is highly likely fraudulent actors could use these phishing panels to steal payment card data, login credentials, and PII from unsuspecting victims.

More broadly, these phishing panels contribute to the rising trend of easy-to-use phishing-as-a-service (PhaaS) offerings that make it dramatically easier for less technically sophisticated fraudsters to carry out phishing campaigns. As these phishing panels can be used to mimic financial institutions, e-commerce websites, and cryptocurrency services, a likely impact of the panels is an increase in the pool of attackers targeting customers of these organizations.

The sources for this report include fraud-focused forums and blogs and the Recorded Future® Platform.

About Recorded Future

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.