Robin Banks might be robbing your bank

ironnet.com/blog/robin-banks-a-new-phishing-as-a-service-platform

Jul 26, 2022

Key points from our research:

- Robin Banks is a phishing-as-a-service (PhaaS) platform, first seen in March 2022, selling ready-made phishing kits to cyber criminals aiming to gain access to the financial information of individuals residing in the U.S., as well as the U.K., Canada, and Australia.
- In mid-June, IronNet researchers discovered a new large-scale campaign utilizing the Robin Banks platform to target victims via SMS and email, with the goal of accessing credentials and financial information pertaining to Citibank, in addition to Microsoft account credentials.
- The primary motivation for scammers using this kit appears to be financial; however, the kit does also ask victims for their Google and Microsoft credentials after they travel to the phishing landing page, indicating it could also be used by more advanced threat actors looking to gain initial access to corporate networks for ransomware or other post-intrusion activities.

Initial Access Brokers (IABs), or criminal actors who sell network access through the form of stolen credentials or initial access tools, have become prolific in today's cyber threat landscape. One very popular tool sold for system access is a phishing kit, provided by phishing-as-a-service (PhaaS) platforms that supply the capabilities needed to carry out a successful attack.

Generally, these kits include sets of files that are pre-packaged to contain all the code, graphics, and configuration files necessary to create a phishing page. This can include features like curated databases of targets or branded email templates, and they're often designed to be easily deployable and reusable. Thus, they provide a quick and easy way for threat actors of all skill levels to gain access to accounts and systems of interest.

Robin Banks: a new PhaaS platform on the market

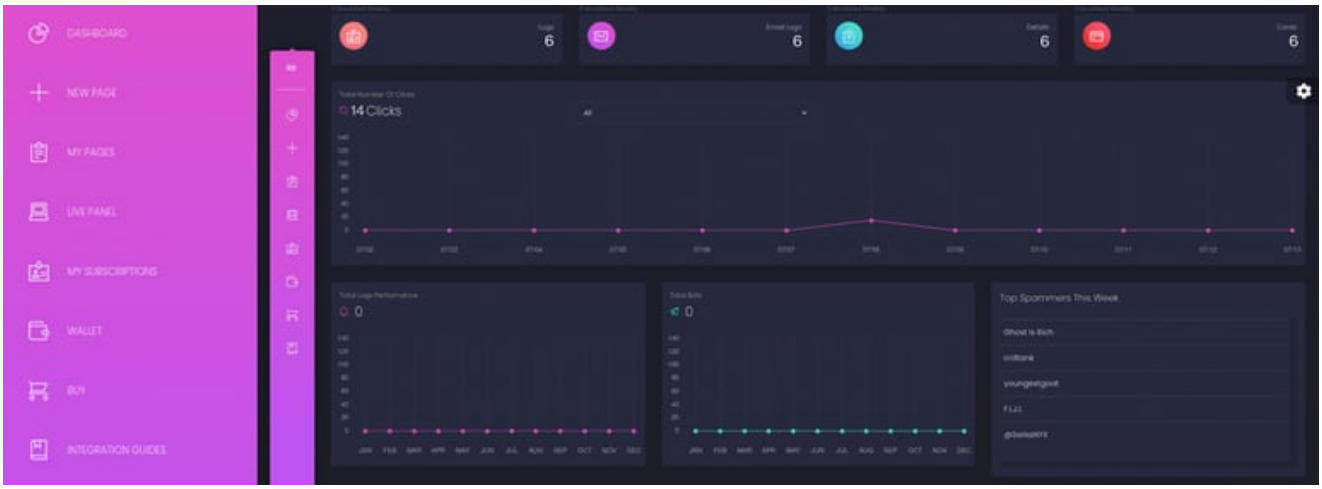
IronNet researchers have recently observed an active cyber crime syndicate launching a new PhaaS platform, selling phishing kits to cyber criminals who specialize in social engineering scams. Known as Robin Banks, this threat actor provides ready-made phishing kits primarily targeting U.S.-based financial companies, as well as numerous companies in the U.K., Canada, and Australia.

Financial institutions advertised on the website include: Bank of America, Capital One, Citibank, Wells Fargo, and more. They also offer templates to phish Google, Microsoft, T-Mobile information, as well as international companies like Lloyds Bank of England, Netflix in Canada, and Commonwealth Bank in Australia.

Based on network traffic analysis and open-source research by our analysts, Robin Banks has been using the IP `5.206.227[.]166` and/or has been active since at least August 2020. The scammer's newest platform, discussed in this blog, has been in operation since March or April 2022.

Accessing the platform

In order for interested buyers to access the `robinbanks[.]in` website, they are required to create an account login with an email and password and to pay via Bitcoin. When entering the site, customers are faced with a well-organized dashboard, offering a sidebar with features to set up a new page, monitor current pages, add funds to the wallet, and more. This is where customers can also access numerous options to craft a custom phishing kit.



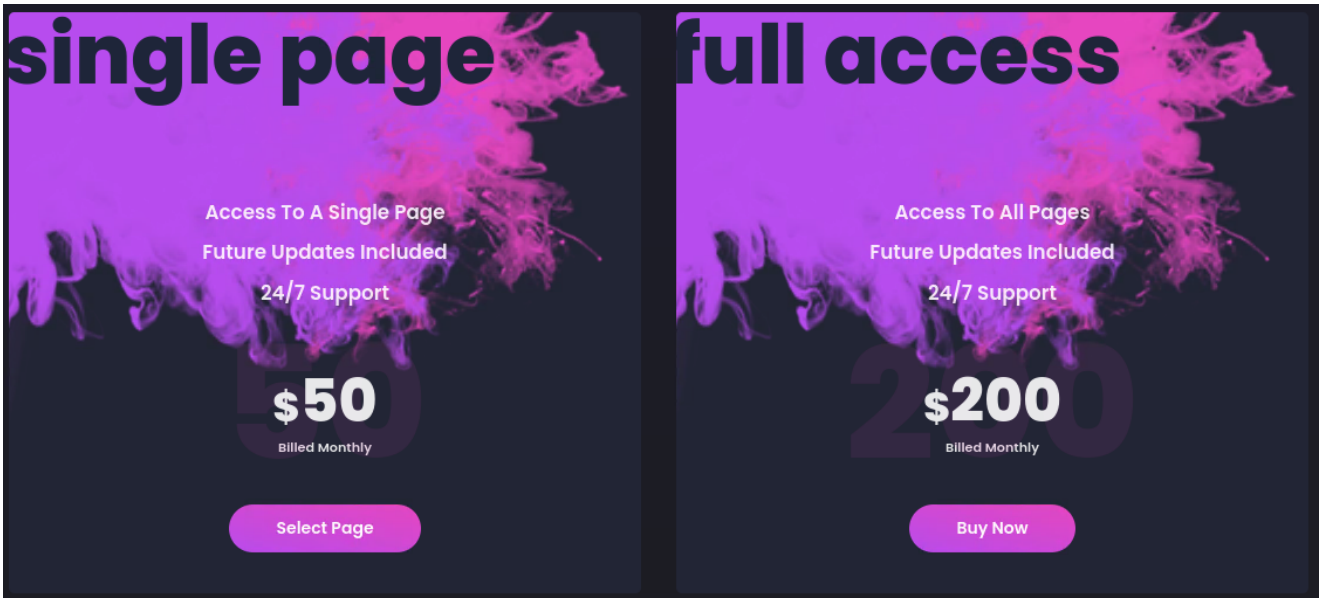
Robin Banks dashboard & sidebar

The Robin Banks website has a more sophisticated yet user friendly webGUI than 16Shop and BulletProftLink — two well-known phishing kits that are also notably more expensive than Robin Banks as well. Over the past few months, Robin Banks has gained many new customers and has been one of the few PhaaS platforms to consistently update templates.

Pricing

Single pages, which include any future updates and 24/7 support, run for $50/month on Robin Banks. For full access, which includes access to all pages as well as any future updates and 24/7 support, Robin Banks charges users $200/month.

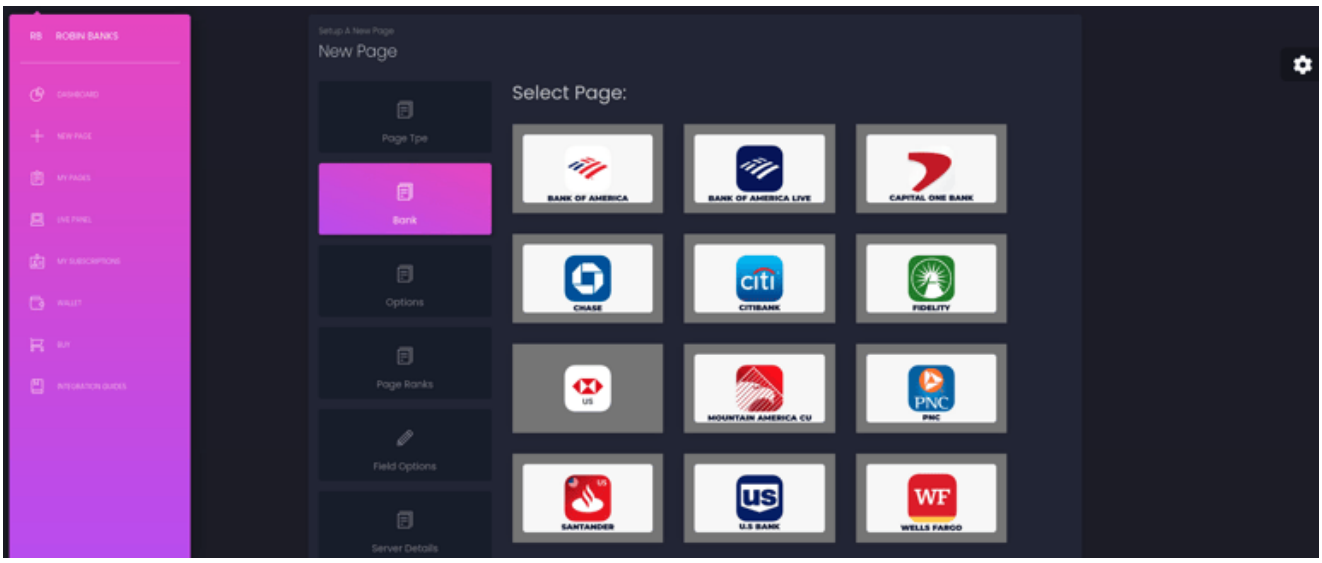
On average, a single kit deployed via a PhaaS provider can cost anywhere between $150-$300/month – sometimes more depending on the services offered.



Robin Banks pricing page

Customizing the phishing kit

In customizing a kit through Robin Banks, threat actors can choose from a myriad of brands to impersonate and target the customers of those brands. Customers have various customization options, such as whether to opt into blocking users based on user agent strings or to employ reCAPTCHA when bot activity is detected.



Crafting a phishing page on the Robin Banks platform

Deploying the phishing kit

Upon accessing the initial access URL sent through a scam SMS or email, the victim will be presented with either the phishing page content or, if the system detects a potential bot, a separate landing page that requires the completion of a reCAPTCHA. This is to stop web scanners from automatically detecting phishing pages.

Once the reCAPTCHA is completed (if required), the victim will then be redirected to the landing page hosting phishing content (landing page is consistently hosted at the domain root with the path `/dfsajsk.php`). The content of the phishing page is hosted both locally to the unique instance and centrally via Robin Banks infrastructure.

As the victim accesses the landing page, their browser is fingerprinted via their user agent string to render content based on their unique device type (mobile vs. desktop). When the victim moves to complete all the form-fields on the site, the domain will then POST all data to the Robin Banks API (hosted at `Rbresults[.]pm / 185.61.137[.]142`).

POST request containing a sample of phished data

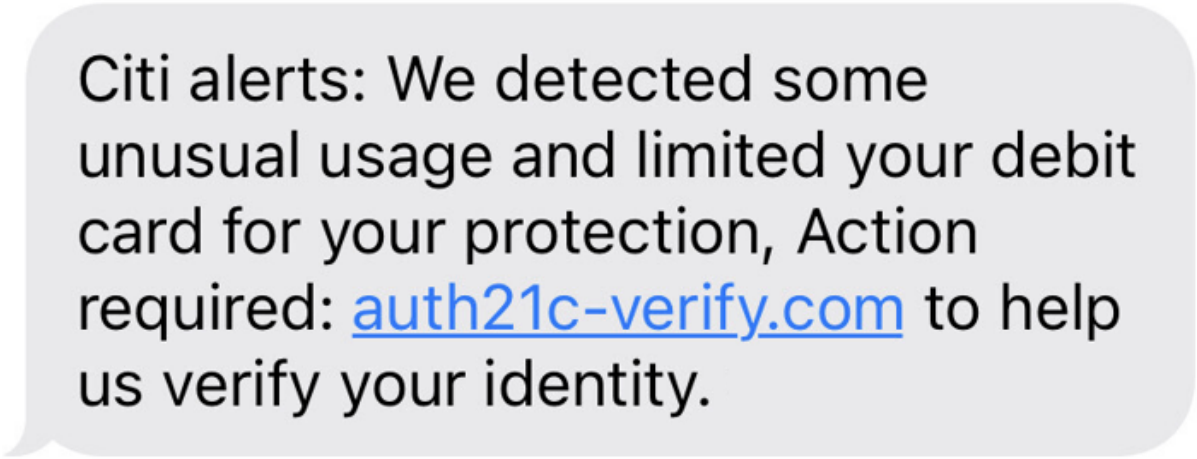
The POST contains two unique tokens: one being the token used by the threat actor to interact with the API/management interface, and the second being the victim.

By analyzing the network traffic, it is clear that the number of POSTs is dependent on the number of unique pages requesting data from the victim. In other words, each time the victim reaches another page requesting information – like their credit card data, CCV, SSN, etc. – a separate POST is created, possibly as a fail safe in case the victim decides to quit the form prior to finishing it.

Once the POST data is sent to the API, it can be viewed in the threat actors' management interface, where they have the option of instantly sharing the data to their personal Telegram channel. Since the data is sent to the Robin Banks API and thus resides on its infrastructure, not only is the threat actor able to view stolen data, but also the administrators of Robin Banks as well.

Case Study: Investigating an active phishing campaign utilizing Robin Banks

In mid-June 2022, IronNet researchers observed a large-scale campaign using the Robin Banks phishing kit, targeting victims via SMS and email. The goal behind this campaign was to access credentials and financial information pertaining to Citibank, in addition to Microsoft account credentials.



Example of phishing attempt from this campaign

Based on investigation of the threat actor, this campaign proved very successful. Numerous victims had account information sold via the dark web and various Telegram channels.

Recently, IronNet researchers have observed this threat actor attempting to expand their campaign and increase its effectiveness. This includes purchasing additional phishing kits from Robin Banks – in addition to the kit they already have targeting Citi-Bank users – to target the customers of other companies. It also includes efforts to diversify their hosting platforms by utilizing a myriad of services such as AWS, Microsoft, DigitalOcean, Oracle, and Google, as well as Cloudflare services. And, aligning with a trend seen with other Robin Banks scammers, the threat actor behind this campaign was observed utilizing Dynamic DNS (DDNS) to diversify network traffic.

Motivation of threat actors using the Robin Banks PhaaS platform

Threat actors using this phishing kit tend to target the basic user, with the goal of making as much of a profit as possible. The primary motivation for using this kit appears to be financial, based on the kit's main functional purpose of stealing banking credentials and other financial information.

Cyber criminals using the Robin Banks kit often post the monetary data of their victims on Telegram and other various websites, listing the hacked account balances of various victims. Some users even use Telegram to resell phishing kits they purchased from Robin Banks.

Through analyzing open-source intelligence and various forensic artifacts, IronNet researchers were not only able to identify potential suspects behind the platform itself, but were also able to calculate the estimated amount of money threat actors have had access to using the Robin Banks PhaaS platform.

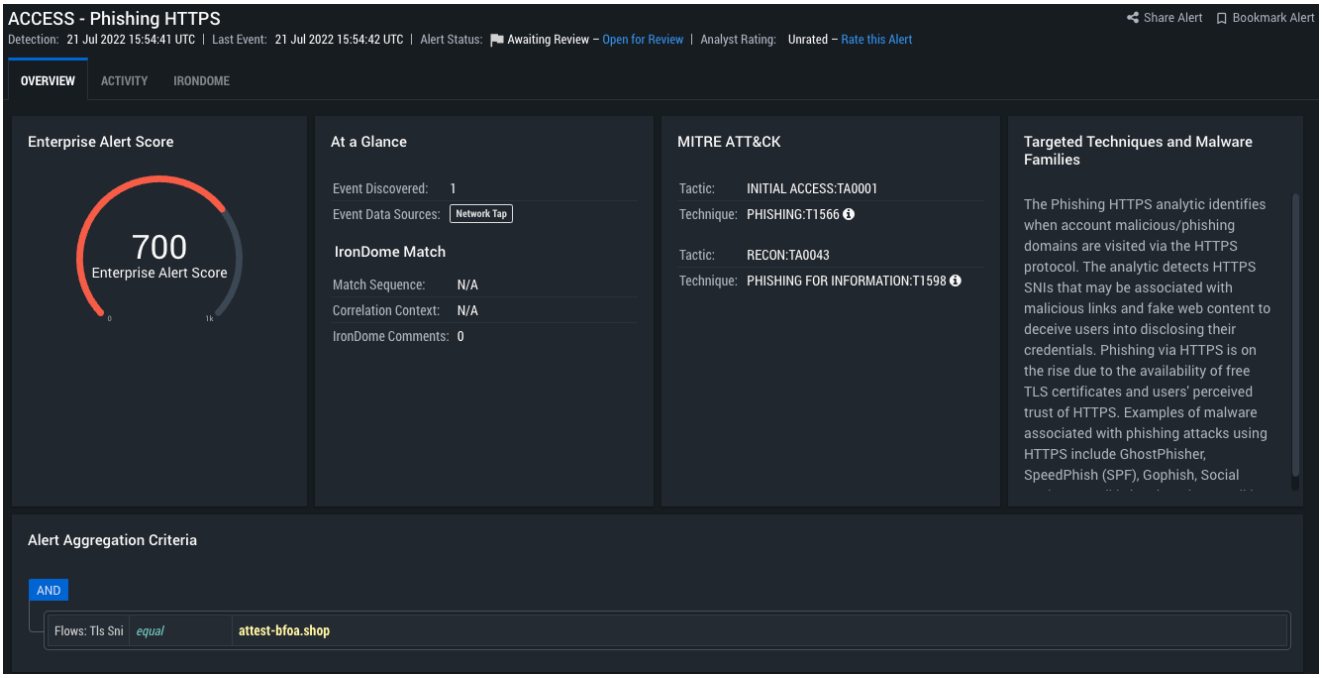
We assess that through the various phishing campaigns utilizing Robin Banks kits, criminal actors have had access to a surplus of over $500,000 – an amount that is rising daily.

Notably, the kit does also inquire users for their Google and Microsoft credentials after they travel to the phishing landing page, indicating it could also be used by more advanced threat actors looking to gain access to corporate networks for ransomware or other post-intrusion activities.

How IronDefense defends against Robin Banks

IronNet's network detection and response solution, IronDefense, includes Phishing HTTPS, Domain Analysis, and Credential Phishing behavioral analytics that protect against this kind of activity.

- Our IronDefense Phishing HTTPS analytic works to specifically identify communications with phishing domains that are employing targeted brand imitation via HTTPS, as well as flag any time a user appears to be interacting with a phishing link or submitting sensitive information to a suspicious external entity.
- Our Credential Phishing analytic identifies when account credentials are transmitted to external destinations via the HTTP protocol.
- Our Domain Analysis analytic also flags activity that could indicate phishing by evaluating outgoing communications from an internal host to a new or unusual domain.
- In addition, Threat Intelligence Rules (TIRs) have been created for all IOCs and deployed in all IronNet instances.



IronDefense Phishing HTTPS detection of an active phishing page utilizing Robin Banks

Conclusion

The purpose of this research is to shed light on a previously unreported PhaaS platform that is being actively used by cyber criminals to attack users, steal account credentials, and more. With phishing being one of the most used tactics by threat actors to gain initial access, it is increasingly important to uncover and monitor PhaaS platforms, such as Robin Banks, that facilitate cyber attacks on a mass scale.

Overall, Robin Banks is just one of many platforms selling phishing kits on the market right now. It is not more sophisticated or widely used than other PhaaS platforms, but it does stand out for the 24/7 assistance it provides to customers and its distinct dedication to pushing updates, fixing bugs, and adding features to its kits.

Given the criminal operator's clear dedication to managing and improving the platform, we suspect the threat actor behind Robin Banks to change tactics or toolings as a result of this report. This could include attempts to modify attack infrastructure, alter the platform domain, change customer permissions, or add new phishing kit features as an effort to make them more evasive.

IronNet Threat Research will be releasing a second blog on the Robin Banks platform in the near future, providing additional IOCs, data, and analysis from our researchers.

Mitigations for phishing attacks

In order to protect yourself and your organization from falling victim to a phishing attempt, you must take a multi-pronged approach. This includes:

- Don't click on links sent through SMS and email, especially if asked to access your account or enter your credentials.
- Use a password manager to ensure the use of unique credentials across all accounts.
- Enable multi-factor authentication (MFA) for all accounts.
- Require phishing training for employees and other partners.
- Monitor and analyze network traffic to detect suspicious activity, such as is done by IronNet's IronDefense platform.

Other MITRE ATT&CK® mitigations for phishing:

- M1049 Antivirus / Antimalware
- M1031 Network Intrusion Prevention
- M1021 Restrict Web-Based Content
- M1054 Use anti-spoofing and email authentication mechanisms (Software Configuration)
- M1017 User Training

Relevant MITRE ATT&CK TTPs and IronNet Coverage

ID	Tactic & Technique	IronDefense Analytics	Use
T1566	Initial Access: Phishing	Phishing HTTPS Domain Analysis Credential Phishing	Threat actors using the Robin Banks platform conduct phishing. IronNet's Phishing HTTPS analytic attempts to detect SNIs that may be associated with malicious links and fake web content, and IronNet's Domain Analysis analytic will fire on the newly created phishing website.

IOCs

Admin Server:	Content Hosting:
5.206.227[.]166	Rbpages[.]nl
Robinbanks[.]in	Rbpagev2[.]in
Robinbnks[.]in	Rbresults[.]pm
robinbanks[.]cc	185.61.137[.]142

Network Threat Hunting

Method	Description
GET to `dfsajsk[.]php`	Indicative of comms to landing page
GET to `rbpagev2[.]in`	Indicative of loading content on landing page
POST to `185.61.137[.]142`	Indicative of successful phish
https://urlscan.io/search/#page.url%3Adfsajsk.php	URLScan Search Query

About Ironnet

IronNet is dedicated to delivering the power of collective cybersecurity to defend companies, sectors, and nations. By uniting advanced technology with a team of experienced professionals, IronNet is committed to providing peace of mind in the digital world.

Back to IronNet Blog