Related Insights

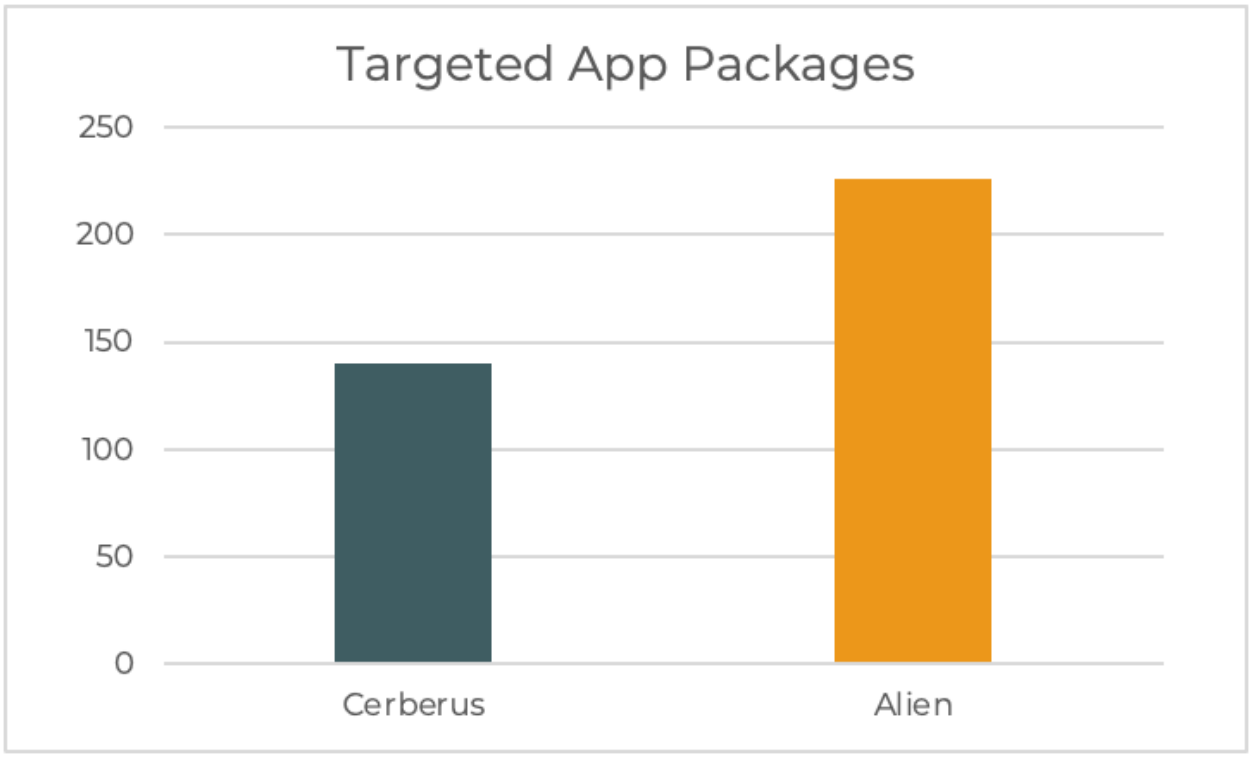
info.phishlabs.com/blog/alien-mobile-malware-evades-detection-increases-targets

May 4, 2021

Get The Latest Insights

By The PhishLabs Team | May 4, 2021

PhishLabs is monitoring the increasing number of mobile applications targeted by the relatively new Alien Mobile Banking Trojan. Alien, a fork of Cerberus, continues to evade Google's malware detection and is targeting a broad spectrum of both financial and non-financial apps. So far, Alien has been connected with 87 new brands previously not targeted by Cerberus.



Cerberus versus Alien Brands Targeted

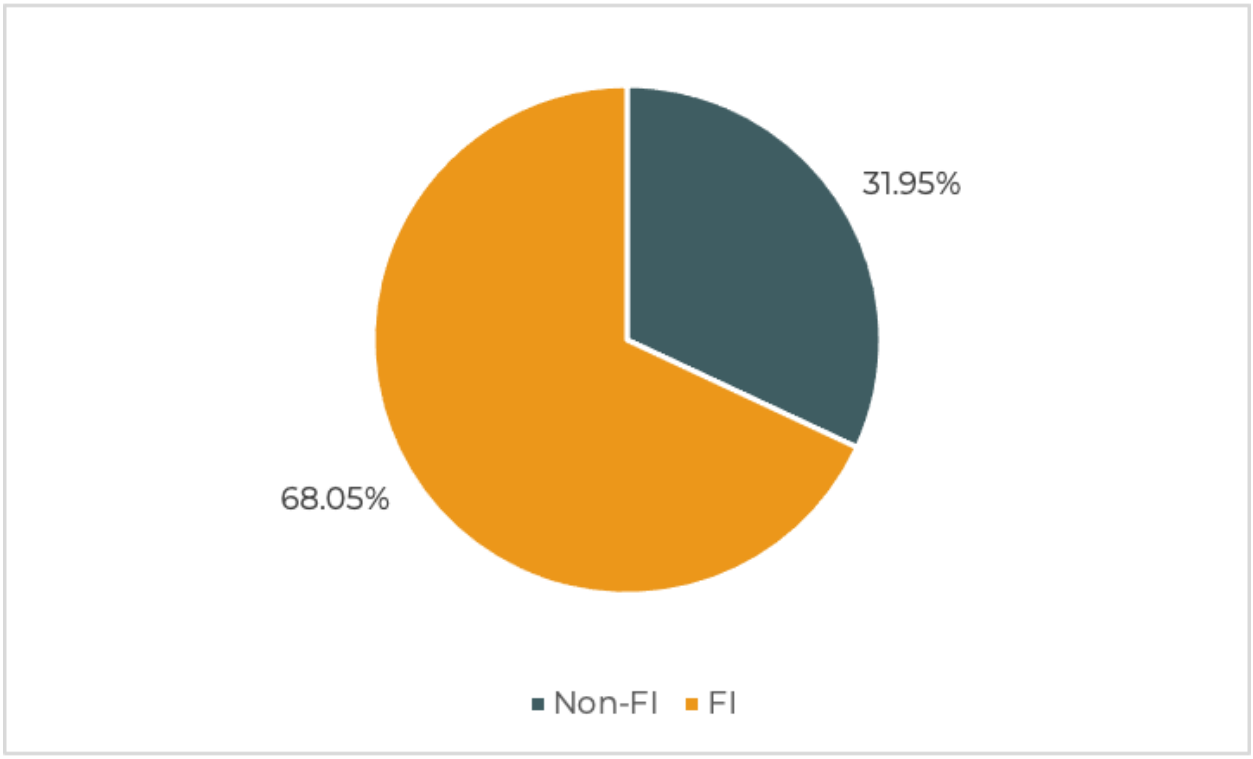
Prior to its decline, Cerberus operators dominated the mobile malware landscape both in functionality and attacks. Cerberus was a malware-as-a-service (MaaS) and targeted 139 known brands during its life.

Since January 2020, Alien has been observed targeting 226 different brands. Alien's high volume of targets may be attributed to its adoption by a growing number of threat actors eager to take advantage of desirable enhancements that increase the success of executing fraud. It also uses a MaaS approach with built-in features that can achieve a wide range of objectives.

Specifically, Alien has capabilities not previously seen with Cerberus, such as the ability to install and navigate Android's TeamViewer. Using TeamViewer gives the operator full remote control access to the infected device, as well as the ability to change device settings, interact with applications, and monitor user behavior.

Alien authors have also incorporated a notification sniffer that allows access to all new updates on infected devices. This includes the ability to steal tokens from Google's Authenticator application, enabling actors to bypass two-factor authentication security measures.

Alien does possess the features originally associated with Cerberus, including keylogging, SMS harvesting, and dynamic overlays.

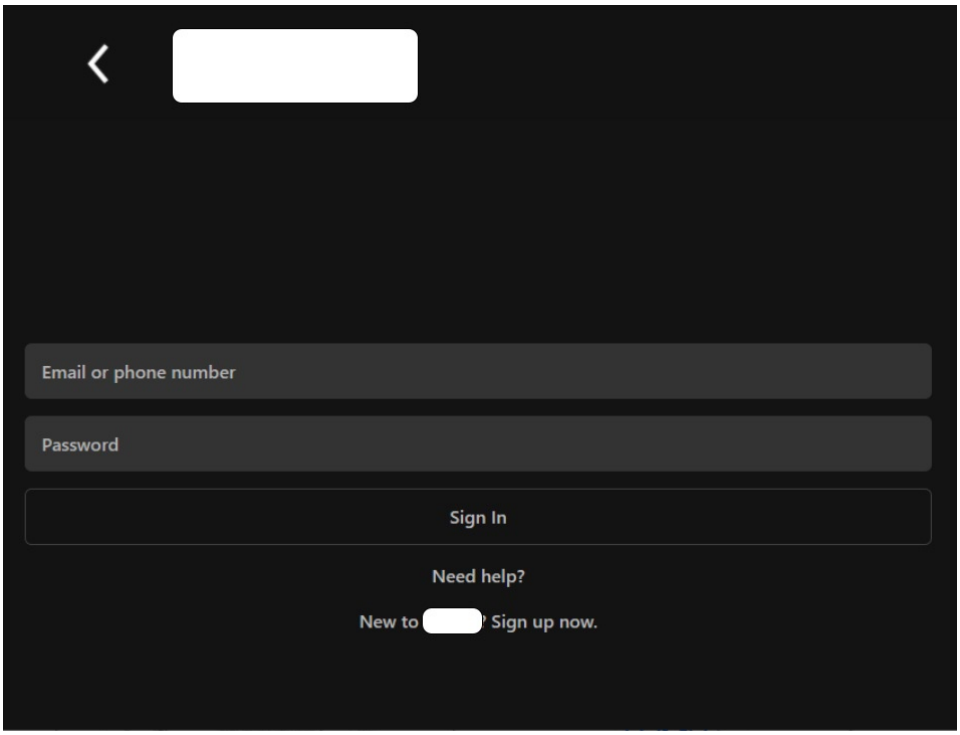


Financial Institutions versus Non-Financials Targeted by Alien

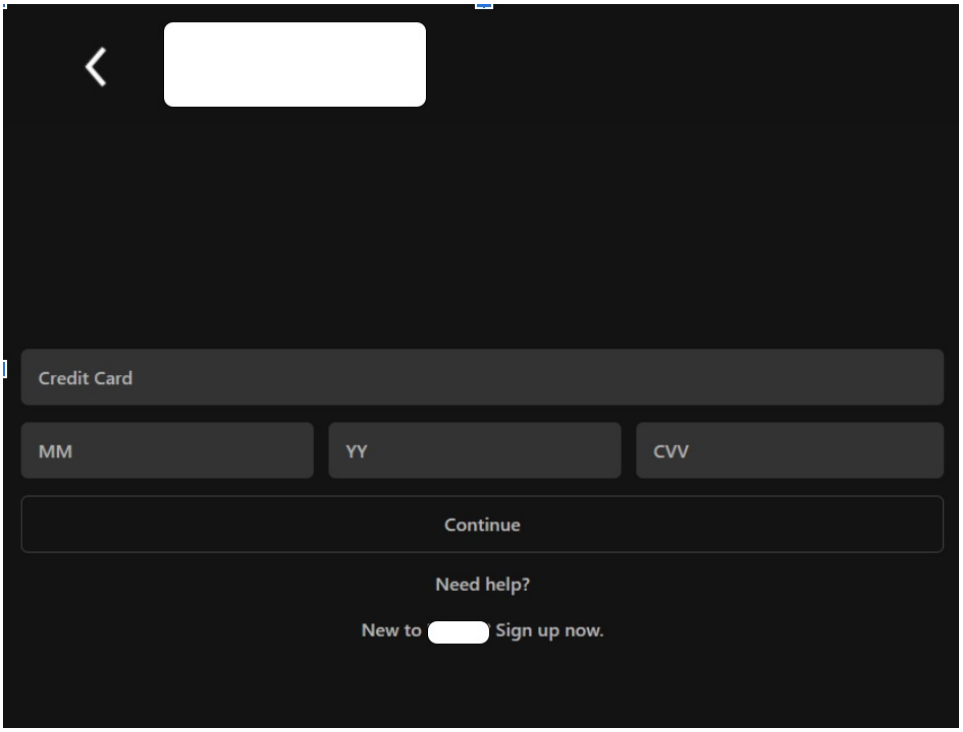
Notably, we continue to observe Alien being used to target an increasing number of non-financial institutions compared to other mobile and desktop malware. This approach boosts the effectiveness of Alien distribution by taking advantage of how individuals may be less vigilant when interacting with non-financial applications not traditionally associated with fraud.

While there is inherent value in capturing email credentials, Alien operators are using custom overlays with dynamic targeting to increasingly capture financial credentials from non-financial apps. Operators are able to pick their desired targets from a list of installed apps sent by the infected device, then supplant the actual application on the screen with an overlay. This overlay is customized HTML code that resembles the target app and elicits payment or identity verification from the victim.

Below is an example of Alien operators impersonating a popular video streaming service to steal both email and credit card information.



Fake Customer Login Page

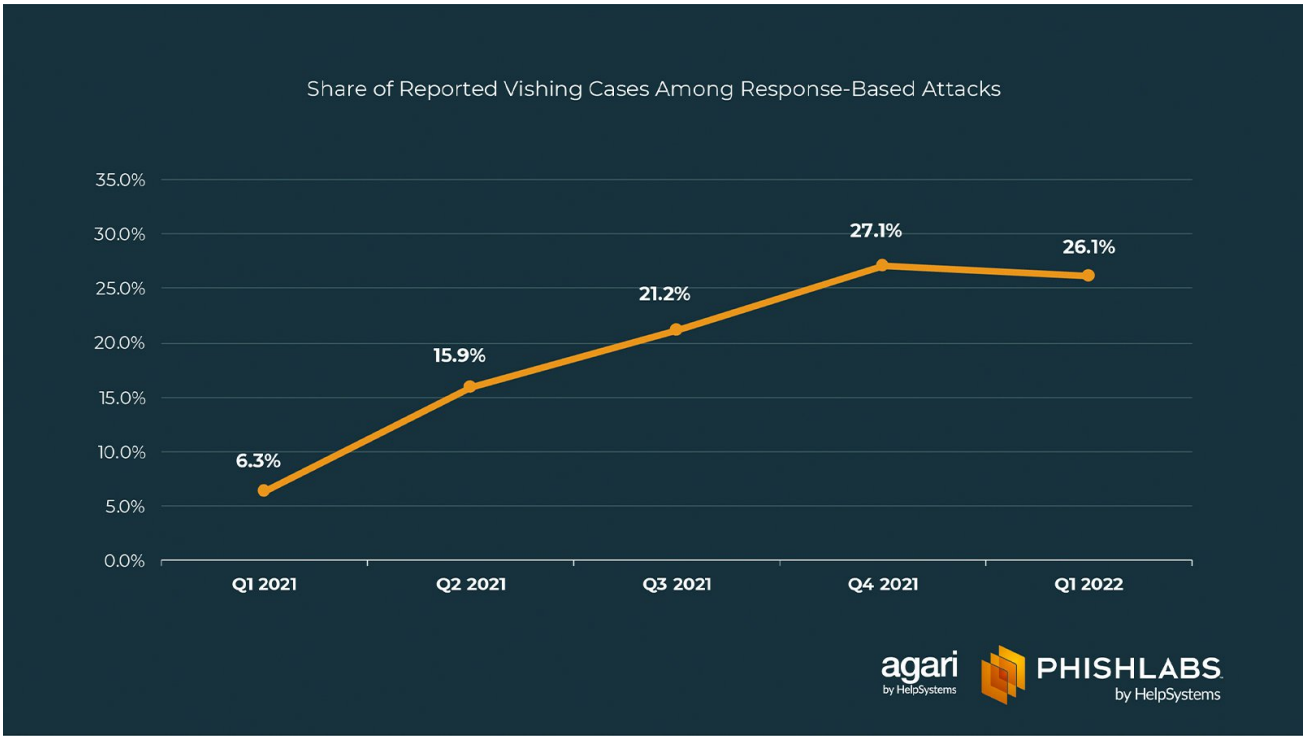


Fake Credit Card Entry

Alien's enhanced features and broader targeting capabilities appear to be making it the mobile MaaS of choice for threat actors. As long as it continues to evade Android's security controls, we expect adoption of Alien to continue increasing.

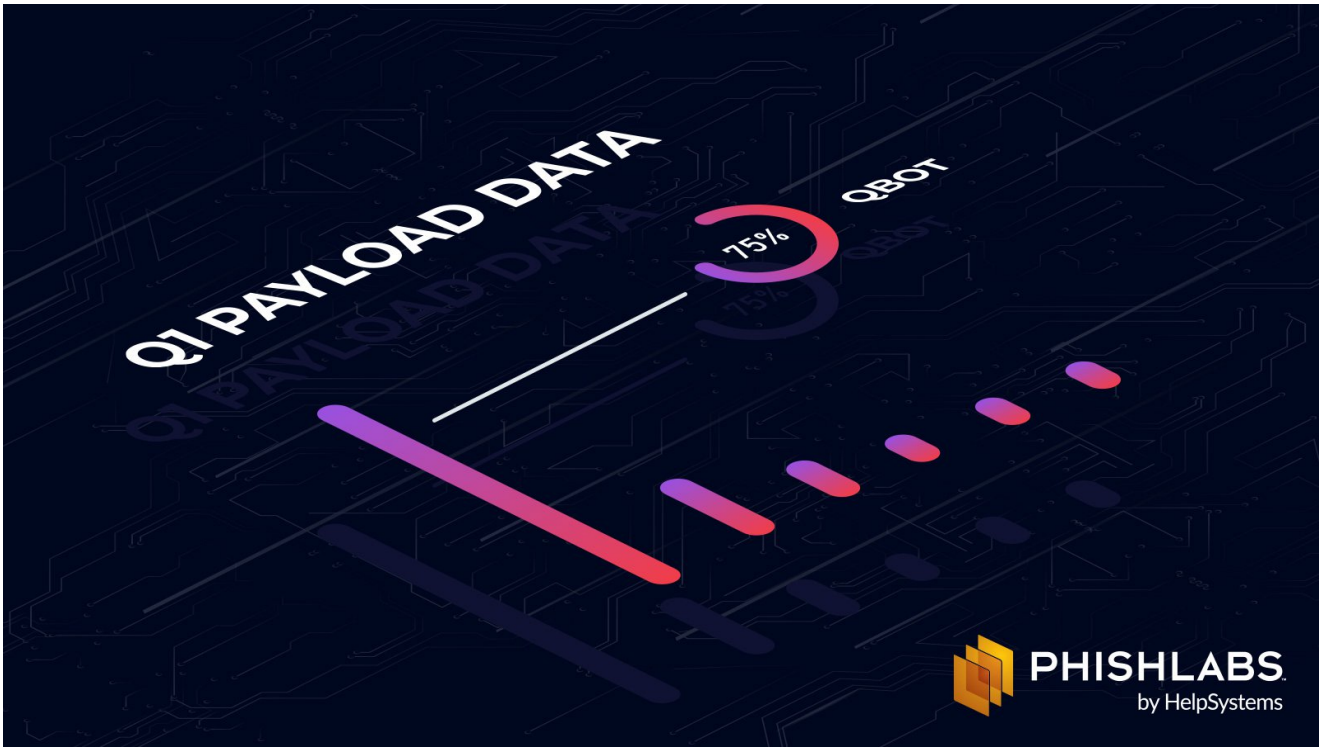
PhishLabs can help organizations protect against mobile malware threats such as Alien. Learn more about Digital Risk Protection Solutions.

Additional Resources:



Vishing Attacks Are at an All-Time High, Report Finds

Vishing attacks have increased almost 550 percent over the last twelve months, according to Agari and PhishLabs' Quarterly Threat Trends & Intelligence Report.



Qbot Payloads Dominate Q1

Qbot payloads targeting enterprises contributed to almost three quarters of all email-based malware since the beginning of 2022.

What is the HelpSystems Value Proposition for Cybersecurity?

In this guest blog, Dr Ed Amoroso, CEO, Tag Cyber, provides a high-level overview of the HelpSystems cybersecurity portfolio value proposition based on a mapping of its component solution offerings to the NIST Cybersecurity Framework (CSF) phases.