**November Dark Web Report**

**October 13, 2023**

**Executive Summary**

This security report documents the results of dark and deep web (DDW), Virus Total (VT), and publicly accessible GitHub repositories, AWS S3 buckets and Azure blobs analysis conducted by a Threat analyst, including crawl or post dates within ~ the previous 30 days. Based on our analysis process and searches conducted, we identified the below company and/or user data indexed or available within our data sources or found in other repositories.

**An important caveat:** While it is important to understand that our research is comprehensive, the nature of the deep and dark web surfaces make the amount of searchable sensitive content still somewhat limited or requires a financial transaction to receive the full content being advertised. We provide full sourcing information for every identified artifact and are always open to more focused requests based on the information we surface through this process.

The Threat analyst identified several key findings that should be evaluated for the potential risk impact including the following:

• ‘Russian Market’ marketplace listings potentially offering compromised access to a monitored network resource.

• Telegram channel posts and Mega file shares possibly disclosing compromised credentials utilizing a monitored email domain and possibly for unknown third-party services.

**Dark Web Analysis**

The following results were identified in data sources leveraged by the Threat analyst. These include results with crawl dates within ~ the previous 30 days. The analysis based on the provided search terms uncovered numerous ‘Russian Market’ listings, and Telegram channel posts, and Mega file shares likely disclosing compromised user credentials for unknown third-party service.

**‘Russian Market’ Marketplace Analysis**

Threat analysts identified 96 ‘Russian Market’ marketplace advertisement referencing a monitored network resource. The network resource was specifically found in an infostealer log advertisement, which are Trojans designed to gather information from victim hosts and exfiltrate it to the malware controller. According to the listing, a Racoon, Redline, Vidar, silencer, or lumma infostealer implant was likely used to capture the advertised log.

In 2023, the ‘Russian Market’ is among the most popular log markets, based on volume of listings available for sale, with an average price of $10 per log. Log listings usually include the infostealer malware utilized to capture the credentials for sale. To date, the top infostealers families are Racoon, Redline, Vidar, Meta, silencer, and lumma. Infostealers allow threat actors with few resources or little technical knowledge to cheaply deploy and capture credentials that can be easily monetized. This type of malware is commonly sold as a malware-as-a-service offering.

The following includes the truncated details for each ‘Russian Market’ listings analyzed.