**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.

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/30/23 08:06 PM** |
|
|

Stealer: **lumma**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/26/23 05:06 PM** |
|
|

Stealer: **Vidar**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/23/23 04:06 PM** |
|
|

Stealer: **Redline**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/22/23 03:06 PM** |
|
|

Stealer: **lumma**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/21/23 02:06 PM** |
|
|

Stealer: **Racoon**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **market\_russianmarket**  **Mo####yf [Diamond]**  **09/15/23 01:06 PM** |
|
|

Stealer: **Meta**  
 Country: **United Kingdom**  
 ISP: **BT Public Internet Service**  
 Total Resources: **3293**  
 Resources:  
 other-sample-domain.com  
 web.sampledomain.com  
 folder.other-sample-domain.com  
 catalog.sampledomain.com  
 sampledomain.com  
 dir.other-sample-domain.com  
 Price:  **$ 10.00**

**Telegram Analysis**

Threat analysts identified 91 Telegram channel posts likely disclosing compromised credentials utilizing a monitored email domain and possibly for unknown third-party services.

Telegram is a globally accessible freemium, cloud-based and centralized instant messaging (IM) service. The application also provides optional end-to-end encrypted chats and video calling, VoIP, file sharing and several other features. Telegram was first launched for iOS on 14 August 2013 and Android on 20 October 2013.

The following includes the truncated details for the Telegram channel posts analyzed.

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **telegram**  **King\_of\_cracking(1232199721)**  **2023-09-30T20:32:37** |
|
|

Document Name: **9K CORPS COMBOLIST.txt**  
 Document Size: **309.0 KB**  
 Document Content:  
 hope0311@sampledomain.com:hope0311  
 mz\_romeo2007@sampledomain.com:reanne  
 jc18@other-sample-domain.com:x4ivygA51F  
 xean.marbun.034160378@sampledomain.com:Lambok25  
 adm@other-sample-domain.com:c3a77820708f25a708a87a3d43f519b8007a8ccfc9344505909  
 candmstathers@sampledomain.com:Michelle09!  
 hs-inoue@other-sample-domain.com:inosachi  
 ayumi0922@other-sample-domain.com:38180922

**Mega Analysis**

Threat analyst identified six Mega file shares likely disclosing compromised credentials utilizing a monitored email domain and possibly for unknown third-party services.

Mega is a cloud storage and file hosting service offered by MEGA Limited, a company based in Auckland, New Zealand. The service is accessed using either a web-based or mobile app. Data on MEGA is end-to-end encrypted. The Web site and service was launched on 19 January 2013, as a successor to Megaupload, which was then seized by the United States Department of Justice.

The following includes the truncated details for the Mega file shares analyzed.

**Findings:**

|  |  |
| --- | --- |
| Source:  Actor:  Crawl Date: | **hosting\_meganz**  **anonymous**  **09/27/23 03:49 PM** |
|
|

Document URL: **https://mega.nz/file/kvVWiIhB#fsZRXVzEWNrTPjK6Rv2sUfwRCKux7QiS\_XoenCnTj3k**  
 Document Name: **[megacloudshop.top] 10k valid\_45.txt**  
 Document Size: **339.8 KB**  
 Document Content:  
 g39es0lig3@sampledomain.com:Eno2ejhrcx  
 hh000068@other-sample-domain.com:62813000  
 qiguangcai@sampledomain.com:6843223214  
 sebal7@other-sample-domain.com:1Q2w3E4r5T6-y  
 matt@other-sample-domain.com:slatwall  
 lsm@sampledomain.com:lourdes  
 hnwph21@other-sample-domain.com:Anyima1141910#