**\_\_\_\_\_\_ \_\_ \_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_ \_\_ \_\_\_\_\_\_ \_\_ \_\_ \_\_ \_\_ \_\_**

**/\ \_\_\_\ /\ \\_\ \ /\ \_\_ \ /\ == \ /\ \/ / /\ == \ /\ \\_\ \ /\ \ /\ "-.\ \**

**\ \\_\_\_ \ \ \ \_\_ \ \ \ \_\_ \ \ \ \_\_< \ \ \_"-. \ \ \_-/ \ \ \_\_ \ \ \ \ \ \ \-. \**

**\/\\_\_\_\_\_\ \ \\_\ \\_\ \ \\_\ \\_\ \ \\_\ \\_\ \ \\_\ \\_\ \ \\_\ \ \\_\ \\_\ \ \\_\ \ \\_\\"\\_\**

**\/\_\_\_\_\_/ \/\_/\/\_/ \/\_/\/\_/ \/\_/ /\_/ \/\_/\/\_/ \/\_/ \/\_/\/\_/ \/\_/ \/\_/ \/\_/**

**Artezza Sharkphin By Benjamin Jaros and Madeline Susemiehl**

**Goals:**

**Even with the best spam filtering systems, it is inevitable that eventually malicious emails will enter an organization. Once a malicious email is identified, Sharkphin enables 365 administrators of all skill levels to quickly search the organization’s mailboxes for similar messages and safely remove them from the environment before they can be opened and prevent further messages from the same source. Sharkphin accomplishes this by offering a straightforward interface that utilizes PowerShell to bring multiple security actions together. Without Sharkphin, administrators would need to manually login to various pages in the Security and Compliance portals to accomplish the same tasks, costing additional time and risk that other users will open the malicious package.**

**Training and Distribution:**

**The EXE package allows the script to be easily transferred to new computers or sent to new members of the support team who may have little to no experience running PowerShell scripts. While caution should always be exercised when removing data in bulk, Sharkphin is configured to soft-delete spam messages. This reduces the risk of an analyst accidentally removing important information permanently, while still empowering a fast and meaningful first response. While this interface makes security actions more readily available, it is always the responsibility of the administrator running the tool to understand the implications. It is of course recommended that a more experienced technician shadow a help desk analyst running the tool for the first time before asking new help desk members to run the tool on their own.**

**Features:**

* **0.2.1**
  + **Create a content search (Compliance Center feature) given the sender and subject of a malicious message**
  + **Monitor the progress of the search and offer to delete the items found in the search**
  + **Add a malicious domain to the tenant Allow/Block List (Security Center feature)**
  + **Add a malicious email address to the tenant Allow/Block List (Security Center feature)**

**Proposed Features:**

* **Additional search options**
* **Add file hash to block list**
* **EML analyzer**

[**An open-source project from Artezza.io**](https://artezza.io)