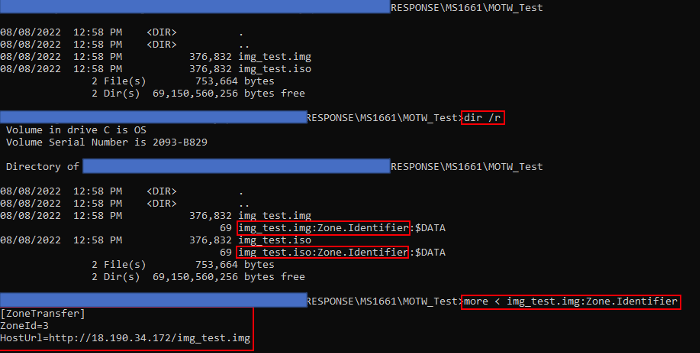
Malicious actors are always seeking new techniques and approaches to gain a foothold into networks. One of the tried-and-true methods, phishing, continues to be utilized as a primary method. Recently, my company has seen in uptick in phishing attacks that contain attached malware. However, instead of attacking a single person, the attackers have pivoted to sending emails to support shared mailboxes with targeted subjects, based on the perceived use case. This has brought about some interesting new malware that left my team very intrigued by how it was able to evade initial detection by our EDR solution.

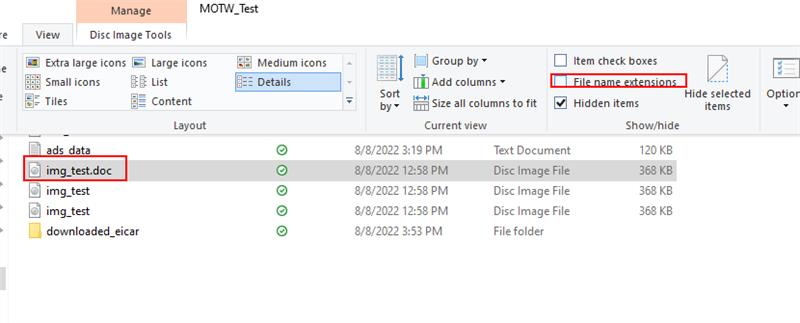
The method of exploit/bypass this specific malware took is interesting. While using an IMG file, it was able to bypass some of the security mechanisms used for downloaded files; <https://attack.mitre.org/techniques/T1553/005/>. Within about two weeks, we encountered two different versions of the same attack, with one utilizing an approach that interacted with the user and a follow-up that was able to deploy silently. Additionally, the first phishing email that was sent on each of these attacks was able to bypass the O365 machine learning and analysis. However, multiple other attacks with the same payloads were detected and quarantined before getting to the end users’ mailboxes. Before getting into some of the analysis, we, as a company, certainly evaluated the need to allow users to send and received ISO/IMG files going forward. We expect this is a temporary fix, and the malicious actors will pivot to another approach.

The following is some of the analysis and events that led up to the detection and termination of the attack chain.

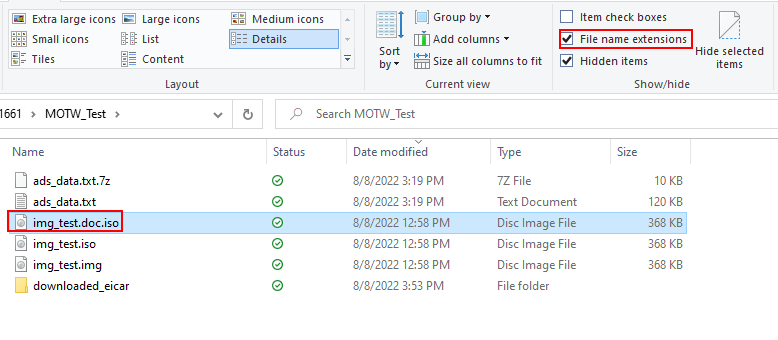
The initial download of the file was not detected as malicious, and it was able to place a zone.identifier ADS on the files, similar to the following:



It was not until the user interacted with the document, a .pdf.img file that an EDR alert was triggered, based on behavioral actions taken with powershell. The user was most likely not able to detect that this was an odd file, due to a setting in their file explorer when they went to go open what they thought was a supporting doc file to a case submitted via the shared mailbox.

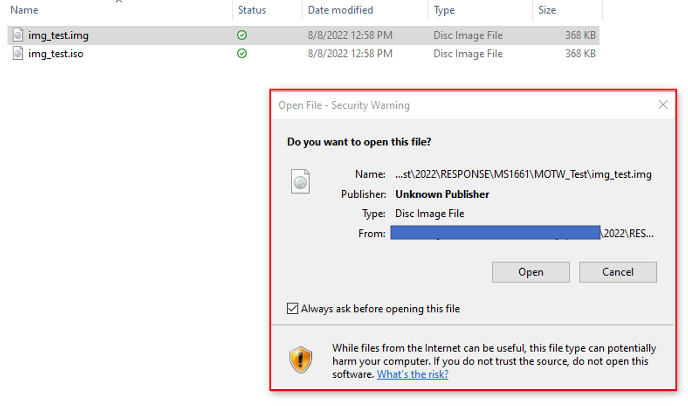


If the user had configured their system to show file extensions, they may have noticed that this was an iso image. However, since they did not notice this, they clicked to open and started the deployment of the payload to the system.



At this step, the user clearly was not paying attention on this strain of malware, as it did pop up a warning for them to accept the actions. A few days later, second train of malware came through that was able to bypass this pop up. In this attack, with the same initial config as the first, the ADS was not written to the files contained in the IMG/ISO containers, allowing them to execute without running. And because these files were not detected by the EDR solution, the malware execution was able to download the IMG/ISO containing the malicious files and mount them without being detected.

Initial malware popup:



What was ultimately detected by the EDR was a powershell command that called out to a website for additional files. In this case, the malicious command reversed the address to attempt to bypass search and detect mechanisms. Because this was not a normal action (running powershell) for this user, the EDR was able to detect and stop the attack at this point in the chain.

