Threat Actors Exploiting Tax Season

eFile.com, an IRS approved software service, was recently found to be delivering JavaScript malware. The service was a conduit for the filing of more than 66 million tax returns in 2022. The malware was loaded on nearly every page of the website prompting users to click on the malicious file to download. Additionally, a new phishing campaign called TACTICAL#OCTOPUS has been observed targeting individuals in the US filing taxes with seemingly valid tax forms. The lure documents observed contained employee W-2 tax documents, I-9, and real estate purchase contracts. These lure documents are sent as an attachment to an unsuspecting victim containing malware with stealthy AV evasion tactics, layers of code obfuscation and multiple C2 (command and control) channels. A phishing email with a .lnk file is delivered to the target using tax-themed lures. While this is a common tactic used in phishing campaigns ,the threat actor has shifted from using encoded IP addresses to using publicly available URL redirect services. Additionally, the PowerShell and VBScript code used are unique and sophisticated, especially from an AV avoidance and obfuscation standpoint making this campaign important to watch. For further information on this threat actor please reference [CS-SU-23-0102] Situation Update - Tax Phishing Campaigns.

As threat actors are becoming more intricate in impersonating various corporations and web services, users must refrain from clicking on redirect links or opening email attachments from untrusted senders. Businesses should continue to educate their employees on social engineering operations and phishing campaigns to increase vigilance when opening emails.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.darkreading.com/application-security/efile-tax-return-software-malware
2. https://www.securonix.com/blog/new-tacticaloctopus-attack-campaign-targets-us-entities-with-malware-bundled-in-tax-themed-documents/?&web_view=true