BumbleBee Downloader Now Being Distributed via Malicious Ads

In early 2023, the threat actors behind the BumbleBee malware shifted to a new delivery method, opting to use malicious online ads to spread the downloader. First observed in March 2022, BumbleBee is a sophisticated downloader that has primarily been distributed via phishing attacks. However, recent activity shows it's being spread through malicious Google ads or SEO poisoning, specifically trojanized installers of popular business software such as Zoom, Cisco AnyConnect, ChatGPT and Citrix Workspace.

This shift in delivery methods may be aimed at remote workers looking to install new software quickly on their home set ups. A simple web search results in fake download pages, which can be difficult to spot, and trick victims into installing the BumbleBee payload. In at least one instance, it was discovered the Bumblebee malware would infect devices even without clicking an ad, as simply loading the webpage with the malicious ad would also load the malware. After initial infection, Bumblebee has historically dropped Cobalt Strike, Sliver, and Meterpreter as a means for threat actors to maintain persistence before conducting ransomware attacks.

Implementing policies that restrict employee privileges to install software and run scripts on their computers can help mitigate this type of threat. Additionally, businesses should ensure software installers and updates are only downloaded from known and trusted websites.

___

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.secureworks.com/blog/bumblebee-malware-distributed-via-trojanized-installer-downloads