Threat Group Cards: A Threat Actor Encyclopedia

Description(Palo Alto) The actor used the BumbleBee webshell to upload and download files to and from the compromised Exchange server, but more importantly, to run commands that the actor used to discover additional systems and to move laterally to other servers on the network. We found BumbleBee hosted on an internal Internet Information Services (IIS) web server on the same network as the compromised Exchange server, as well as on two internal IIS web servers at two other Kuwaiti organizations. As mentioned in our prior xHunt Campaign blog, we still do not know the initial infection vector used to compromise the Exchange server, as this appears to have occurred prior to the logs we were able to collect.
