Arkadiy Kantor

Reconnaissance assignment

Target: ENCLARA

Enclara is a mail order pharmacy and pharmacy benefit manager (PBM) focusing primarily on hospice care. The company has grown significantly recently due to several mergers and acquisitions. The mail order model provides comprehensive pharmacy support, delivering medications directly to hospice patients’ homes, with the backup of local pharmacies to serve their same-day and emergency needs. While the PBM model allows a hospice to “pay as you go” for the resources they utilize and get medications processed locally.

The CEO is Andy Horowitz and the public facing website provides pretty extensive bio’s for the leadership team. This can provide a great social engineering opportunity and makes it easy to find and identity these people online by name and cross referencing their education/work history. The company has several IT positions available but the descriptions focus mainly on soft skills and don’t share a lot of technical knowledge. One particular position appears to have Win2k and Server2k under technical requirements. Since those products have been out of support for so long they can potentially be threat vectors if any more information about these systems can be identified, assuming they are still relevant.

A whois lookup appeared to match the address and phone number for the company, however the name is still under one of the previous companies “excelleRx, Inc” (pre merger) no individuals are listed as contacts and a generic email address is given. There are no ARIN entries. The Nmap command helped me discover that the website is running on IIS 8 and windows Server 2012. Otherwise they was not much else of interest.

The most significant thing I noticed is that the public website contains 5 different client log-ins for various services that are offered. This opens the door for many more opportunities for recon and potential threat vectors. Gaining access to any of those sites would potentially expose the personal information of many patients. Both the client and Enclara could be liable for any patient breaches. I would recommend doing a better job of securing the individual portals and making the log-in pages private and/or putting them behind a firewall.