2024

Advocate: Lutheran General Hospital

RECONNAISSANCE

PENNIE, JOHN

PENNIETESTING | 1 E. Jackson Blvd.

Table of Contents:

Executive Summary:

After conducting this exercise, I have found so much information that I surprised myself. Obviously, it helps a bit that it is a relatively large hospital but from using tools from the lab I found a lot more. But even without technical knowledge, people with power and privileged access are far too easy to find, as they should be since their officials that affect everyone in the hospital. But in my opinion while Byrnes, the CIO, LinkedIn looks nice it gives off much more information than Ahuja, the COO, who to me is much more secure. You'd think the Chief Information Officer would want more privacy as she should know how information can be used such as her face and name. Not to mention the security, physical and cyber, is lackluster at best; when security should be paramount for a hospital that generates millions of dollars and sensitive patient information. But then again, the healthcare industry is all about money and gaining personal information, when it should be about nothing but helping sick patients and preventing risk to others health. I would be willing to bet most of the "security professionals" at this institution would fall victim to a seemingly legit phishing attack generated by AI, but hey I should give them more credit, right? Most of the time security professionals aren't even targeted by threat actors, usually it is high ranking individuals that aren't concerned with the all-powerful device in their pocket or underpaid sanitation workers and/or interns.

Overview:

I chose Advocate Lutheran General hospital (LGH), as this was the hospital I was born at twenty-two years ago and my dad works for as contractor through Advocate. I also find it interesting since it is a hospital and takes care of hundreds of patients a day, yet it is only Advocate 10th largest hospital. Advocate Aurora Health is a nonprofit organization that was recently in hot waters for trying to merge with another large healthcare provider but was shut down due to the fear of forming a monopoly. After some brief digging, I found that Advocate doesn't have a dedicated CSO or Soc Analyst, neither are they looking for one. The closest thing I was able to find is the current Chief Information Officer (CIO) who is for the entirety of Advocate. I've also been able to find Ip domains dating back to 2008 (16 years ago) and everything in between. Additionally, I find hospital cybersecurity especially interesting since the hack about a year ago that took down a lot of hospitals include Lurie Children's; interestingly enough, LGH fell victim to a data breach in 2021 (almost exactly 3 years ago). To me this is very interesting as it wasn't even a remote breach, a person stole a laptop containing sensitive patient information which should be the easiest thing to control and protect. Luckily, they had the laptop setup so that the laptop was a paperweight after leaving the premise.

Findings:

Surprisingly, after conducting my reconnaissance, I have found a lot more information than I originally anticipated. I have been able to find 70+ Ip domains associated with Lutheran General, just from searching their site on SecurityTrails. These domains date back to 2008, and Advocate, nor LGH own/host these domains outright. Their previous domains were hosted by GoDaddy, Microsoft, Team Internet, Aptum Technologies, Google, and Amazon to name a few. It was also quite easy to find their "local data center" which is located across the street in a strip mall, its conveniently named "Lutheran General Hospital EMS office" on Google Maps. More surprising, I was able to find their internal documentation highlighting how to connect remotely to their site with several hyperlinks going to login pages. One of these login pages was even outdated in terms of copyright since 2016, while the other had no copywrite information at all. I also searched for their current ips (15.197.148.33 & 3.33.130.190) on Shodan.com, which returned reassuring information: only ports 80 and 443 are open on their active ips. But I found some confusing information such that it looks like several other sites are sharing the domain (orchardlaw.com, refimyhometoday.com, and xavantmusic.com). Finally, there have been a few data breaches since 2016 (most notable for paying a record $5.5 million HIPAA fine) where customer data was leaked and sold, as well as less concerning the theft of a hospital laptop in 2021, that was fortunately bricked after leaving the premises. Weirdly enough, they hired a new CIO after the most recent breach in 2016. The public address for the hospital is 1775 Dempster St, Park Ridge IL 60068; while the address for the local data center is 8816 Dempster St, Niles, IL 60714. I was only able to find this due to it being listed on Google, not from Ips, all of those go back to mostly Seattle and California (some other older outlier states like Louisiana).

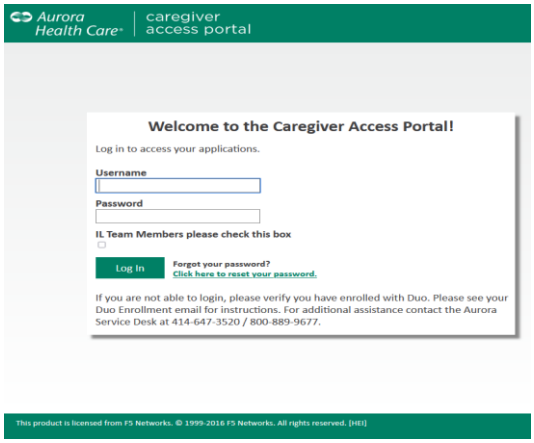
Extrapolation of Findings:

While most of the information found on the previous page is hardly harmful in most hands, the right threat actor with the right motive can do anything they put their mind to. With that being said, in my opinion there is far too much information out there for this hospital for my personal liking. Nonetheless, there is enough outdated information that it makes it slightly difficult to find accurate and relevant data. I also do not like the fact that the CIO oversees all Advocate hospitals and also there is no dedicated Soc Analyst or even a CSO. Also, in my opinion the current CIO has little to no expertise in cybersecurity when it comes to reviewing her LinkedIn, (but it may not be her full comprehensive background), which is still alarming. While currently they use AWS for their hosting, the email hosting is seemingly provided by Microsoft Outlook. If someone who is novice in foot-printing can find this much information, I can only wonder what an expert can find. While we're not tasked or allowed to try and gain access I believe with some social engineering and/or exploits I could gain access to servers and/or privileged information. I'm not sure if this is a big deal, but I can easily inspect element and manipulate values on their website; but, from some brief research on SQL and CSS I found that it is extremely easy to restrict access to inspect element and other administrative tools for web hosting. I was able to find the CIO and COO's LinkedIn's very easily; Bobbie Byrne and Deepinder Ahuja. But both have good LinkedIn profiles with very little personal information aside from job experience, nonetheless Ahuja was recently hired as COO as of February 2024 and Byrne as of 2017 (after their biggest HIPAA violation). A non-security individual would find this information very interesting as this is all publicly available and these people can easily be manipulated with little knowhow and a lot of time/balls.

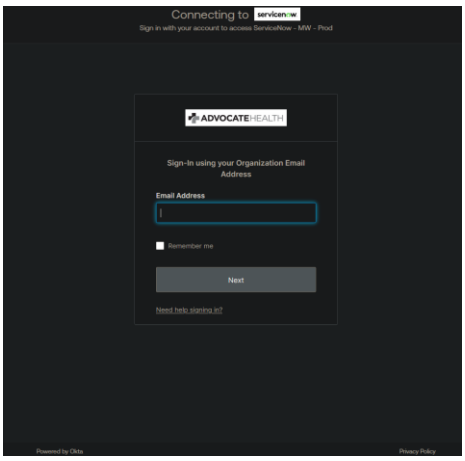
Evidence:

Easy to find PDF outlining remote access:

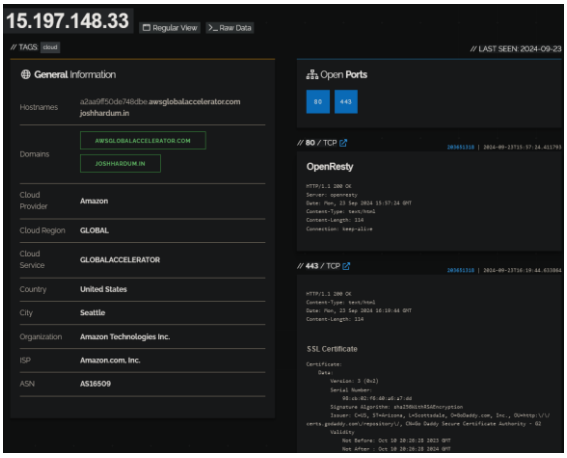
Outdated (2016) Copywrite login:



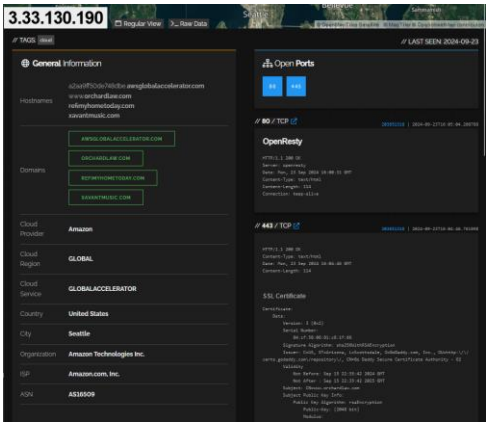
Seemingly secure login:



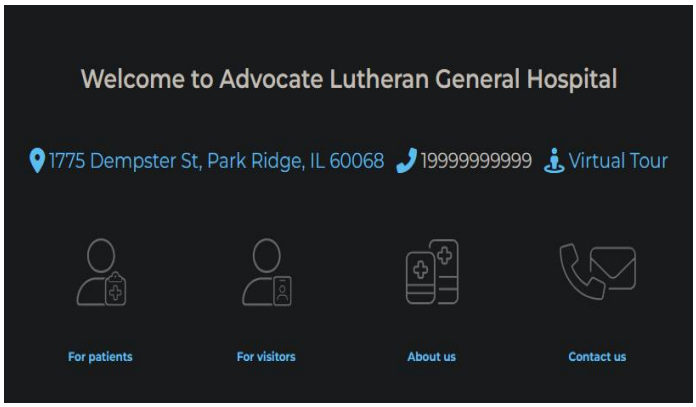
Shodan Review of 15.197.148.33:



Shodan Review of 3.33.130.190:

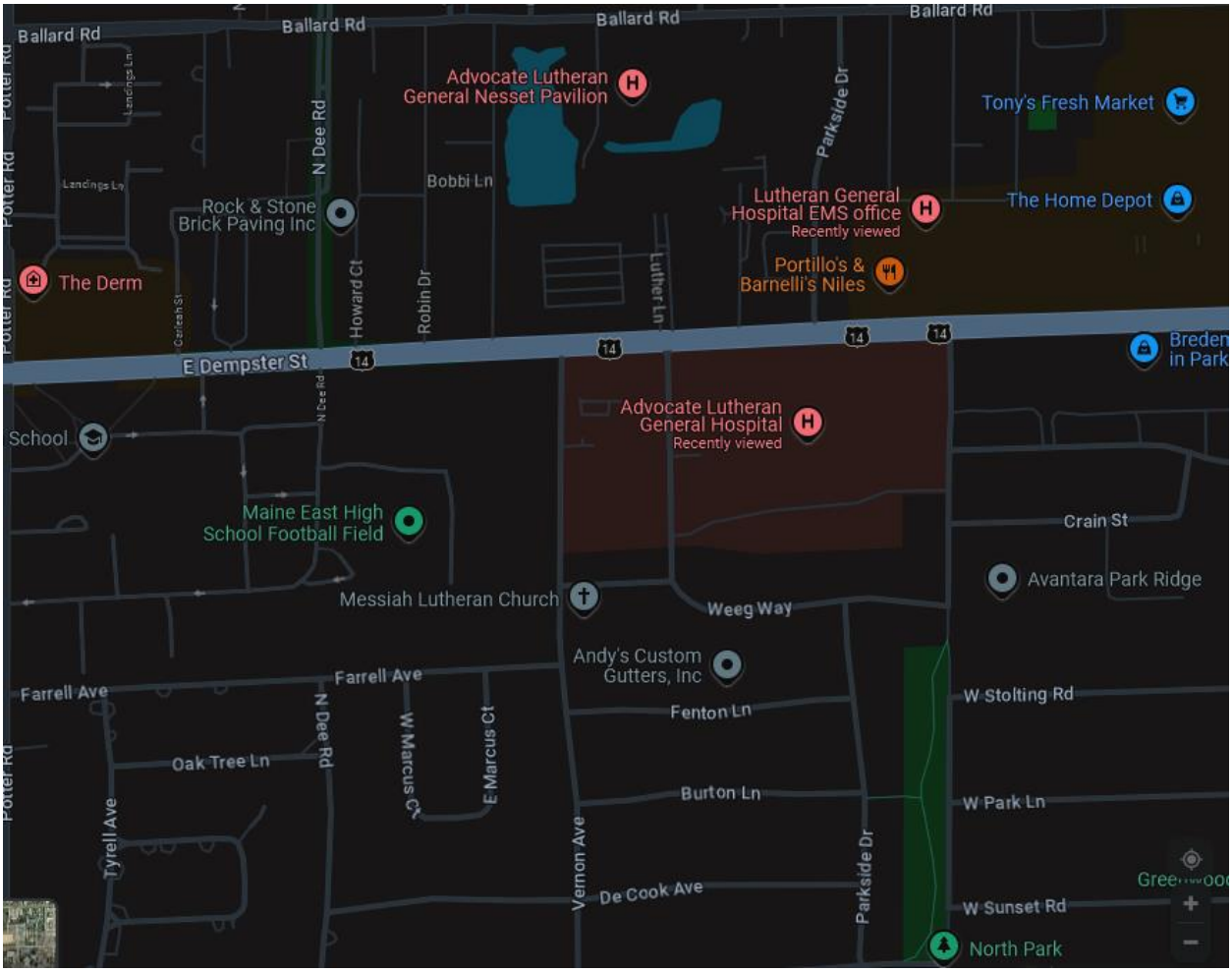


Basic website manipulation(phone number):



Location:

Direct area of all LGH owned assets.



- The public address for the hospital is 1775 Dempster St, Park Ridge IL 60068.
- The address for the local data center is 8816 Dempster St, Niles, IL 60714.
- The address for the outpatient center is 1775 Ballard Rd, Park Ridge, IL 60068.

Works Cited (no particular order):

1. Google Maps, search operators, and general searches
2. https://www.linkedin.com/in/bobbie-byrne-md-mba-0b6b472/
3. https://www.healthcaredive.com/news/advocate-health-appoints-executive-team-merger/638121/
4. https://www.linkedin.com/in/deepinder-ahuja-8a691b47/
5. https://www.advocatehealth.com/covid-19-info/_assets/documents/additional-resources/wi-hit-citrix-storefront-instructions-.pdf (privileged PDF), https://access.aurora.org/my.policy (outdated), & https://atriumhealth.okta.com/login/login.htm?fromURI=%2Fapp%2Fatriumhealth_servicenowmwprod_1%2Fexk9bu48cnKAC0not4h7%2Fsso%2Fsaml%3FSAMLRequest%3DnVJdb9swDPwrht79WSephTiAl2BYsK4zmmwPeykYia6F2pInyk737%252Bs4GZY%252BrBj2St4dj0cuCdom6XjRu1o%252F4M8eyXkvbaOJnzs5663mBkgR19AicSf4rvhyx5Mg4p01zgjTMK8gQuuU0WujqW%252FR7tAOSuC3h7uc1c51xMMQ5GAEOBxpMqAzwNfmGAjThhqGDp4wkIZ5m9GG0nDSu2I7q%252Fq2RmhcHZhnBxMNuu5N5%252FGiO8q2x9OgxzjEl%252Bfs0Ke3Qn8u1pE2Lq0XIZEJTzsy76OxAqcEclZBQ8i87SZnu%252Fv1Yb4QmFUwB5SpjLKZSG%252BrRVXN0ixOJN6MQCqBSA34h0rU41aTA%252B1ylkRJ6keZn9zs4wWfZTydB2PtB%252FPKS3YflJZKP70f9OEMIv5pvy%252F98utuPwkMSqK9H9H%252FkfF3tDTlO%252Bqz1XI6N5%252FM2%252BsPeN8X%252FD47W%252F2LgWV4PeYytOOnDbab0jRK%252FPKKpjHHtcVRImfO9jgdqAX3dydxEE8VJf1qgnJsQTWFlBaJWLi6zH3756tX%26RelayState%3Dhttps%253A%252F%252Fadvocateprod.service-now.com%252Fsp%253Fid%253Dkb_article%2526sys_id%253D07a58aaddb32af4c31b261f74b9619d4 (seemingly secure).
6. security@aah.org (security email).
7. https://careers.aah.org/job/20527688/public-safety-operations-center-telecommunicator-full-time-2nd-shift-park-ridge-il/?source=10588 (job posting for physical security, obviously lackluster).
8. https://www.indeed.com/cmp/Advocate-Aurora-Health/jobs?q=analyst&l=Park+Ridge%2C+IL#cmp-skip-header-mobile (job posting for data analyst and security positions).
9. https://stackoverflow.com/questions/28690564/is-it-possible-to-remove-inspect-element (evidence for easily protecting against inspect element).
10. https://www.shodan.io
11. http://dev.healthitsecurity.com/news/over-68k-advocate-aurora-patients-impacted-by-elekta-health-data-breach (one of many breaches)
12. https://www.chicagotribune.com/2021/09/29/computer-containing-patient-information-reported-stolen-from-advocate-lutheran-general-hospital-police/ & https://databreaches.net/2021/09/29/computer-containing-patient-information-reported-stolen-from-advocate-lutheran-general-hospital-police/ (stolen laptop)
13. https://www.advocatehealth.org/about/leadership/ (leadership)
14. https://whois.arin.net
15. https://securitytrails.com (used to find all associated Ips and domains).

16. https://www.advocatehealth.com/luth/ (base website) www.lutherangeneral.com