CxO Trust Newsletter - August 2021

Jim's CEO Intersection

Hi All,

We hope that you are enjoying this new newsletter, part of CSA's CxO Trust Initiative. It is always great to receive feedback to make sure we are addressing your needs. Please let us know if there is any information we could include that would be useful to your mission.

I thought I would share with you my experiences at DEF CON 2021, with BlackHat the first major in-person cybersecurity conference since RSA 2020, right before the pandemic lockdown. I know many of you are struggling with corporate travel policies, especially with the rise of the Delta variant of COVID-19. Las Vegas is one of the hotspots for the Delta variant and has instituted mandatory indoor masking. DEF CON added mandatory vaccination as a requirement to attend. I cannot speak for everyone, but my vaccination card doesn't have anything on it that looks authoritative and for the most part was filled out by myself as per the process where I was vaccinated (State Farm Stadium in Glendale, Arizona). So while the card could easily be faked, everyone seemed pretty serious about it, as well as masking up, so overall COVID protocol compliance was very high in my estimation. Seating for the tracks was standard chair setups without social distancing and everyone was jammed together like a normal conference. The labs, vendor area and other activities were more spaced out, likely a function of a smaller crowd than normal years. I am terrible at estimating crowd size and it was held in 2 adjoining hotels, but I will guess around 8,000. I have not heard of any reports of COVID infections from DEF CON a week later. I am not making predictions, but Vegas was very busy and if an event like this can be held safely in the ultimate party town without attendees getting sick, that will be a good sign for all of us. Here are a few of sessions I attended:

- Ransomware Policy Panel - This panel had some great experts of note, including Chris Painter, co-chair of the DOJ Ransomware Task Force. It is no reflection on the experts convened, but there was a lack of solutions and even a consensus of the steps forward. It shows how difficult this problem really is. A couple of experts had even confessed to having converted from a "never pay ransom" position to "some victims have no choice". Large companies with state of the art cybersecurity programs can manage this challenge with data tiering strategies, business continuity planning and overall cybersecurity hygiene. My takeaway is that organizations with a low to moderate level of cybersecurity sophistication and a lot of on-premise infrastructure are at the most risk. This is likely one more reason for the cloud for these companies, I think it would be good for CSA to work with cloud storage companies on guidance around maintaining data storage archives to make ransomware demands moot.
- Phishing with AI - A team from Singapore showed how AI as a Service is going to make phishing and ransomware even more lethal. This group has been testing AI services, they are getting cheaper and better. The result is that phishing messages will be more believable and malicious attackers will be able to scale attacks upward and deploy more rapidly.
- Using 5G & LTE infrastructure for Covert Channels - I loved this presentation as the technique was so simple and elegant that I can't believe I haven't seen it before. It was shown how anyone could use cell towers to broadcast their own messages by using MAC-layer contention protocols. It reminded

> me of the Independence Day aliens (“they are using our own satellites against us!”). It was noted that there could be positive uses for this vulnerability as the infrastructure could allow messaging even if the network was down. Resilience.
>
> - Using a Drone as a Flying Exploit Kit - This was fun for me, because I have been predicting for years that this would be used to compromise targets in a specific location, even if they were air gapped from the Internet.
> - Swedish Central Bank Digital Currency Proof of Concept - This attempt to prototype an e-Kroner by the Central Bank using Corda tools was interesting and showed many challenges in the state of art. The implementation so far is prone to corruption in many ways. Transaction chains can be created to a size that the back end processing infrastructure crashed. Also, “Transactions of Death” could be crafted to send to users and put their currency in a permanently unusable state. Lots of work to do here.

As we start thinking about practical research CSA can provide for CISOs within this initiative, one area I would like to knock out is knowledge baselines of cybersecurity and cloud security for boards of directors. What is the baseline of knowledge we can define for all directors and what is the baseline for directors hired for their cyber knowledge? Ponder that and let me know what you think.