Anonemis Research
2016-2022 Cyber-Breach Report

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Anonemis Research
2016-2022 Cyber-Breach Report

Cyberstalkers who purchased my public data and installed spyware to incept text messages with the intent to annoy. There has been interference with competitors as well as adversaries.

  - **What was done to mitigate the impact or recover?** The goals in these attacks where inconvenience and annoyance. I notified affected parties and went on with business as usual. Recovery was mitigated in this manner due to the motive and nature of the attacks: Passive and non-retrieval of relevant data or established threat.
  - **Recovery:** I conditioned attackers to maintain their own logging in the location of the cyberattacks. Maintaining a log of their own daily offensives and in the event of an unlikely escalation in attacks, data is already logged and stored. However, the intention and overall goal isn't monetary but validation, therefore the log will suffice while also acting as an active net for similar attacks which have been also common. Otherwise known as, copycats.
- **Have you or has anyone you know experienced any disruptions or impacts due to a cybersecurity issue, whether by nature or due to a specific attack?** Yes, however, the agent was non-reactive. This was unintentional but a perfect response that maintain the uniformity of not validating the attacks but keeping them at bay and consumed within their system logging.
  - **How bad was it?** This had been ongoing; amateur. However, there was a non-specific mental health impact on those who had been victimized.
  - **What type of event was it?** Hacking, Passive Attacks, Cyberstalking, discriminatory and predatory driven attacks.
  - **What things helped to remedy the situation?** Invalidation. This was and is an attention seeking crime and although, escalation is possible, because anything is possible within cybersecurity, it is unlikely, and therefore the net logging has proven to be effective. The less reactive on the enterprising end the more control is maintained of the overall response operation. The more data available or logged increases a larger more sustainable conviction within the judicial system.
    - They have become more familiarized with this cyberspace and are immediately reactive as a subconscious response due their compulsion conditioning.
    - This leaves digital trails, shows which content has been edited and when it was first created. It's logging, timestamping, patterning, locating, and creating an informal criminal transcript associated with each user and their digital patterns. Thus, in the event of a crime which requires immediate reactive responding, there is digital log of the who, what, when, how and where.

        - **What types of issues made it worse?** Trial and Error: distinguishing which team members could thrive under pressure and which ones could not.
    - **Identify at least three types of IoT devices in your home or in the home of someone you know.**
    - iPad
    - Rumba
    - Ring
    - Headphones
    - Cellphone {Bixby other application}
        - **Do they have secure passwords?** No.
        - **What harm, if any, could occur if an attacker took control of the system or device?** Eavesdropping.
- **What specific cyber threat(s) pose(s) a significant challenge to your environment and why?** Sextortion, Cyberstalking, Doxing, Hacking Kidnapping and Blackmail. Malware, Phishing, Spamming and socially engineered attacks.
- **What other types of malicious attacks have you witnessed or been privy to?** Failure of Sextortion, Kidnapping and Blackmail, Hacking and Doxing.
    - **If known, what type of attackers were associated with the attack (for example, cyber criminals, script kiddies, nation-state, etc.)?** Cybercriminals: International.
- **What response mechanisms or countermeasures do you think would help address this/these specific threat(s)?** Employing an automated system which baits cyber criminals, logs the crime, formulating data transcript to be forward on to cyber law enforcement operations.
    - **What mitigation measures would you implement, or what actions would you take?** Achieving major prosecution within the confides of these specific crimes, perpetrators and perfecting an automated system which operates independently but is overseen by qualified and trained agents.
- **What preventative measures or security tools would you generally prefer to use to address this threat?** The cyberspace currently works as bait net, so inducing more traffic would be the ultimate goal to ultimately achieve more arrests and preventing any further copycats. Writing bills which protects users and prosecute offenders to the highest standard.