**The Shadow Brokers**

The Shadow Brokers is a mysterious hacker group that first appeared publicly in summer 2016. The group is known for stealing a few disks full of National Security Agency (NSA) secrets in 2013 and dumping those secrets on the internet since August 2016 (Schneir, 2017). The dump included exploits and tools collected, hoarded, and used by the NSA hacking group Tailored Access Operations (TAO) (Armerding, 2017). Consequently, the group was successful in publicly embarrassing the NSA and damaging its intelligence-gathering capabilities. The dumps were also effective in exposing major vulnerabilities in Cisco routers, Microsoft Windows, and Linux mail servers forcing these companies and their customers to scramble (Schneir, 2017).

Among other things, the Shadow Brokers also provided the exploits that the authors of the WannaCry ransomware used to infect an estimated amount of 400,000 computers in more than 150 countries. This launch is known for being the biggest ransomware outbreak in history. After the WannaCry outbreak, the Shadow Brokers threatened to release more NSA secrets every month, giving cybercriminals and other governments worldwide even more exploits and hacking tools. Certainly, the NSA had wanted to keep all of the exploits caused by the hacker group secret and only to be used for the agency’s surveillance purposes. However, it has been used by criminals (Armerding, 2017). Since they first appeared, the Shadow Brokers had published four sets of NSA material. These include exploits and hacking tools against routers, network devices, mail servers, and Microsoft Windows. The group released all the content uncensored. They also posted anonymous messages in bad English but with American cultural references (Schneir, 2017).

Lastly, it is known that the Shadow Brokers requested a minimum of one million Bitcoins, which is more than $500 million for their exploits, which they were selling at auction. However, no one seemed to be interested in purchasing these cyberweapons. Hence, it doesn’t look like the group made big money, which was apparently one of their goals. Nevertheless, the hacker group and Russia are considered to be behind the release of the cyberweapons and are likely to be the sole owners of the leaked NSA tools (Burgess, 2016).

References

Armerding, T. (2017). Shadow Brokers cause ongoing headache for NSA. Nakedsecurity by SOPHOS. Retrieved from https://nakedsecurity.sophos.com/2017/11/15/shadow-brokers-cause-ongoing-headache-for-nsa/

Burgess, C. (2016). NSA’s Tools Go Missing to Shadow Brokers. ClearanceJobs. Retrieved from https://news.clearancejobs.com/2016/08/22/nsas-toys-go-missing/

Schneir, B. (2017). Who are the Shadow Brokers? The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/