B5 An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder

Christopher W. Day, BS, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131*

After attending this presentation, attendees will understand a typical Persistent External Targeted Threat (PETT) attack and one of the most common follow-on modes of persistence utilizing stolen, but valid, network access credentials. Previously, PETTs were most commonly observed in government agencies but are now becoming more prevalent in the private sector as demonstrated by the so-called "Aurora" attacks against Google in January of 2010. A common result of a PETT attack is the compromise of valid user and system administrator credentials that are then subsequently used by the adversary to continue to access the victim network via VPN, RDP, Enterprise Portals, or other remote access platforms. Due to the fact that the credentials used by the intruder are valid access credentials, the intruder is simply "logging in" and no longer required to utilize an exploit or some other form of "hacking" to continue to intrude into the network. This form of intrusion is difficult to differentiate from legitimate user access and hence challenging to detect.

This presentation will impact the forensic science community by providing practitioners with awareness of this form of illicit activity as well as network and system observables to detect it in networks of interest. Given that one of the primary results of a PETT attack is sensitive data exfiltration, it is important for investigators to know how to identify the patterns and observables that the malicious misuse of valid network access credentials leave behind in the forensic record. Finally, a new free, extensible, open-source tool will be introduced to help investigators process many common log file types to highlight the observable patterns of the above-mentioned malicious misuse of valid network credentials.

Intrusion, Detection, Credentials

 ** Presenting Author*