Op MULLENIZE and beyond - Staining machines 10/10/12

01:13:02 pm, by , 576 words
Categories: MCE, MCD, MISD

Op MULLENIZE and beyond - Staining machines

UK Top Secret Strap1 COMINT

The Problem: A large number of users on one Internet Protocol(IP) address at one time (e.g. in an Internet café) means it is difficult for analysts to identify individual IP addresses or users.

The Solution: Working together, CT and CNE have devised a method to carry out large-scale 'staining' as a means to identify individual machines linked to that IP address. Carried out as Op MULLENIZE, this operation is beginning to yield positive results, particularly in . User Agent Staining is a technique that involves writing a unique marker (or stain) onto a target machine. Each stain is visible in passively collected SIGINT and is stamped into every packet, which enables all the events from that stained machine to be brought back together to recreate a browsing session.

Much of the work in CT operations involves understanding extremists' use of the Internet. Generally, this is achieved by looking through passively collected SIGINT data and using that information to recreate an Internet session, based on what was happening on a particular IP address at a particular time.

The location of collection assets or the telecoms infrastructure of some countries means that the IP address seen attached to each event collected might not be the one actually used by the target to access the Internet. These IP addresses might be servers, proxies or NATs (Network Address Translators – the Internet-facing device in a private network of machines) and they can play havoc with the ability to recreate an internet session for an individual.

example of a region using massive NATs, with thousands of users on one IP address at any one time making it virtually impossible to identify our targets in that country. The idea of large scale staining of machines seemed to present a solution to this problem.

In order to deploy these stains at scale across machines used by the extremist community decided to target machines where the users visited extremist web forums used to deliver the stains to each target machine mechanism that leverages GCHQ's huge passive SIGINT accesses to deliver CNE payloads to targets. As this is a very new approach to tackling a tough target, it took 12 months for policy, collection, processing and CNE issues to be resolved, but after a lot of hard work by some committed individuals across Benhall, Bude and SOUNDER, successful implementation of staining at scale was achieved.

Over 150 stains are now deployed against machines the technique has been adopted to help with work agains with nearly 200 stains deployed there in the last 2 months. Analysis is becoming easier and the benefits are being felt outside of the teams that started the work. An unexpected benefit from this work is that targeting any of the machines that have been stained for further CNE efforts is much easier.

This is a great example of CNE effects enabling passive SIGINT and then this in turn enabling CNE and will hopefully lead the way for future joint projects on hard targets.

If you would like to hear more about the techniques and tools used in Op MULLENIZE sign up for a **Mission News Live presentation** on Tuesday, 16 October.