Infiltration - Successes and Pitfalls of Penetrating Hostile Online Groups

P2P4-W04: Infiltration: Successes and Pitfalls of Penetrating Hostile Online Groups

Lance Cottrell, Chief Scientist, Ntrepid
Few security professionals choose to take control back from their opponents by bringing the fight to their doorstep. However, by working to infiltrate their groups, organizations are better equipped to combat fraud, discover new malware, or look for specific threats. In all cases, researchers and analysts need to avoid identification and the associated risk of blocking or reprisals. In the RSAC 2018 Peer2Peer session *Infiltration - Successes and Pitfalls of Penetrating Hostile Online Groups*, attendees explored various techniques employed, examined which were most successful, and discussed some best practices to stay safe and effective.

The discussion was held under Chatham House Rules, and in keeping with the theme of anonymity, and as such this summary avoids mentioning anything that could be used to identify the participants. The discussion participants included: an analyst for a major consulting firm, a fraud analyst for a major technology company, a researcher for an anti-phishing security company, multiple senior members of corporate security teams, and several individuals from the U.S. Government.

In all cases discussed, participants were conducting these activities to collect information rather than to directly attack or “hack back”. They visited public discussion forums and marketplaces, explored hidden sites on the dark web, lurked on internet relay chat (IRC) channels, and observed public social media activity.

One interesting discussion surrounded the question of whether these actions should be undertaken directly, or outsourced to “grey hats,” who are more familiar with the groups they are observing. After they were recruited through conventional channels, they all passed background checks which suggested that either they had not engaged in criminal activity, or they were skilled enough not to get caught. These contractors worked remotely using their own hardware and network connectivity, leaving the employers with no oversight capability at all.

Lack of oversight was a consistent theme throughout the session. In particular, corporate activities of this sort were completely below the radar of management. There was a sense that ignorance and deniability were desirable on their part and as long as the activities did not infect the network or incite counter-attacks, operators were free to do whatever they felt appropriate. No one on the corporate side worried about violating website end-user license agreements (EULA) or other policies. In sharp contrast, the government participants talked about the level of regulation and detailed auditing required for their activities.

Recent laws that increase liability for websites have created an unexpected problem for the researchers. Previously, a great deal of illegal activity was conducted openly on websites like Reddit, but now many of those public sites have been shut down, and a consensus replacement has not yet appeared. Public and dark web Reddit clones are starting to emerge and provide some good sources of intelligence. Dread <http://dreadcomdopoda.onion> has emerged as one leading location for illicit activity. Many websites specialize in different kinds of criminal activity. Some crimes are punished much more harshly and investigated more diligently than others. This led to the creation of more public sites for less serious
content and a few well-protected spaces for the most risky activities like heroin sales and child pornography.

Most investigators, at least at the corporate level, make due with basic and commonly available tools. Several participants use TAILS <https://tails.boum.org> to ensure any trackers are eliminated from their computers, and several used commercial virtual private servers (VPS) or VPN services to hide their IPs. Many of the participants were concerned about the risk of accidentally forgetting to enable privacy tools, and were very aware of the example of Guccifer 2.0 being exposed by failing to use a VPN just one time. One option to prevent this kind of mistake was to use a VPN with a failsafe mode that blocks all traffic when the connection is dropped. Another option was to use a hardware VPN that automatically protects any device connected to the network behind it.

These simple tools work well for the corporate investigators because the activities are short term, and their opponents are relatively unsophisticated about their defenses. One participant talked about joining a hacker IRC channel and simply lurking quietly for days. The public channel allowed anyone to join, and the operator made no attempt to find long-term lurkers, which could be identified with a very simple script. It was not until the lurker messaged the operator that he drew attention to himself and started a witch hunt. No one from the corporate side had made any attempt to create realistic identities to interact with their targets or secure invitations to closed groups and sites.

The government participants were aware of some more sophisticated activities from their organizations but were not at liberty to discuss them.

For now, the biggest problem for corporate infiltration is finding the places where their targets are having discussions and doing business. As these sites continue to be infiltrated and taken down by law enforcement, it is likely that anyone trying to observe them will need to start taking more precautions and upping their game.