Regional Conflict and Cyber Blowback

web.archive.org/web/20160315044507/https://www.crowdstrike.com/blog/regional-conflict-and-cyber-blowback/

Matt Dahl

October 10, 2013

The Internet has changed many aspects of modern life, from communication with friends to how we watch TV or listen to music. It has also changed the way we engage in conflict with others; this can be seen on a micro level in the emergence of cyber bullying or at the macro level in the declaration by the U.S. Department of Defense declaring “Cyber” a fifth domain of warfare.

Cyber conflict can be an equalizer for adversaries who have limited ability to achieve their goals through other conventional avenues. As an example, take the case of individuals supportive of the Syrian regime; these supporters have little ability to engage in kinetic warfare against Western or anti-regime targets in the physical world, but leveraging cyber attacks is well within their capability.

Over the past three months, the adversary designated by CrowdStrike as DEADEYE JACKAL (commonly known as the Syrian Electronic Army) carried out a number of attacks against major media outlets. In mid-August, reports emerged that the adversary successfully redirected visitors to the major media websites such as the Washington Post to a DEADEYE JACKAL-controlled website; the actor also claimed to have similarly compromised the websites of CNN and Time. Several weeks later, DEADEYE JACKAL successfully took down the New York Times’ website through a DNS redirection.

It is interesting to note that these were not direct attacks against the targeted organizations’ networks; they were carried out by compromising the networks of third-party service providers. These third parties were leveraged by the targets to support social media marketing, content publishing, advertising, and domain registration/hosting. Compromising these vendors is a new tactic for DEADEYE JACKAL, who leveraged it as a force multiplier. This tactic negated the necessity of compromising three hard targets, allowing the adversary to increase impact dramatically by finding a common link and exploiting it. The attacks by DEADEYE JACKAL were clearly motivated by press surrounding the conflict in Syria that was critical of the Syrian regime. This adversary is supportive of the current Syrian regime, and it likely desired to control the messaging it felt was driving international anti-regime sentiment. In general, these attacks were disruptive and did not target sensitive data of the media outlets or service providers. These attacks represent the emerging threat of regional conflicts spilling over into the cyber domain and damaging or embarrassing entities far outside of the conflict zone.

Desire to control messaging about the Syrian regime motivated DEADEYE JACKAL’s targeting of the media; however, they could easily adjust targeting toward more impactful targets. As an example, DEADEYE JACKAL may have similarly decided that Western financial institutions would be an effective target to dissuade kinetic involvement of external militaries. Financial entities in the U.S. have already been victimized by attackers calling themselves the “Cyber fighters of Izz Ad-Din Al Qassam” who purportedly seek retribution for an offensive video posted to a popular video sharing site. DEADEYE JACKAL could also turn its sights on entities within the defense industrial base, as the weapons produced by those companies might be used in a strike against Syrian government forces. Organizations in the oil and gas sector could also be targeted if the adversary views interference in the Syrian conflict as a pretext to secure access to oil resources in the region. Whatever the business vertical one can come up with, there is a potential reason why an irrational actor motivated by self defense might seek to leverage cyber attacks against it.

The spillover of regional conflict is also demonstrated by the activity of another adversary designated by CrowdStrike as CORSAIR JACKAL (also known as the Tunisian Cyber Army). During 2013, this adversary carried out a smaller number of high-profile attacks aimed at organizations in the financial, oil and gas, and shipping sectors. Additionally, in March 2013 the adversary also made unconfirmed claims that it compromised a large user database from a financial institution. Although CORSAIR JACKAL’s operations were not as visible as those of DEADEYE JACKAL, the adversary represents another instance of malicious cyber activity emanating from a tumultuous region directed at organizations that may not have a clear connection to the conflict in that region. In the case of CORSAIR JACKAL, the only legitimacy needed to target Western businesses was anti-Western sentiment from perceived interference by Western governments in theatre.

Organizations across all sectors must consider the risk of conflict in the physical world spilling over into the cyber domain and resulting in malicious actors targeting their systems, operations, or customers. The use of cyber attacks is not declining; it is rapidly proliferating. As tools become easier to acquire, use, and modify, new adversaries are stepping on to the cyber domain from all over the world every day.

It is for these reasons that CrowdStrike advocates an intelligence-driven approach to security; the CrowdStrike Intelligence team tracks adversaries emanating from geographic locations across the globe and various motivations. This past quarter we identified multiple new adversaries with specific Tactics, Techniques, and Practices (TTPs) and associated actionable indicators for our intelligence subscription customers. These new adversaries include the two nationalistically motivated actors discussed above, DEADEYE JACKAL and CORSAIR JACKAL, and a number of others engaged in targeted intrusion operations such as STONE PANDA, NIGHTSHADE PANDA, GOBLIN PANDA, and MAGIC KITTEN.

Learn More about CrowdStrike’s approach to intelligence-driven security.

LISTEN NOW

Register for our 10/16 CrowdCast: “You Have an Adversary Problem. Who’s Targeting You and Why?”

REGISTER NOW