Europe's Hacktivists Set Sights on Political Entities

BLOG | DECEMBER 14, 2017

The tumultuous state of global politics that has come to define 2017 continues to shape the motivations and schemes of a wide range of adversaries. In October, CNBC reported two Czech election websites were hacked and that, after Catalonia's independence referendum was ruled illegal, the website for Spain's Constitutional Court was taken down by a DDoS attack. These are just two of many examples that align with a trend Flashpoint analysts have observed in recent months: the proliferation of hacktivist activity targeting European government and political entities.

In early September, Flashpoint analysts observed multiple hacktivist-fueled DDoS attacks against several websites belonging to ministries and individual public officials in multiple European countries. Although these campaigns have been characterized by DDoS attacks dispersed across central Europe, some actors have tended to concentrate their activity on certain countries. For example, analysts have observed that one Turkish nationalist group appears to be focused on targeting the websites of Belgian and Austrian political entities. This group has also indicated its intent to retaliate against any perceived anti-Turkish or anti-Muslim sentiment emanating from European political entities. In one instance, the group posted screenshots of successful DDoS attacks against Danish government institutions. They claim to have carried out the attacks due to perceived insults by Danish politicians against Islam.

While hacktivist groups are often considered less skilled than their cybercriminal and state-sponsored counterparts, the risks and resulting damages they can inflict are by no means novel. Typically motivated by fundamental and political differences of opinion, hacktivist campaigns have been known to disrupt, deface, or otherwise take down targeted websites, web-based services, networks, and infrastructure. Unfortunately, these types of damages became a reality for many following the recent hacktivist-fueled DDoS attacks that correlated with major 2017 elections in the United Kingdom, Germany, Russia, Czech Republic, and France. It appears that the polarizing effect of these elections continues to contribute to the heightened risks faced by various European political entities.

Flashpoint assesses with a moderate degree of confidence that hacktivist-fueled DDoS attacks against European political entities may continue in the coming months. While addressing hacktivist activity can be complex and challenging, organizations—not just in Europe, but worldwide—that integrate Business Risk Intelligence (BRI) into their security and risk strategies can and do mitigate these types of risks more effectively. By providing proactive visibility into rising geopolitical tensions, emerging hacktivist threats, and upcoming schemes, BRI enables organizations across all sectors to gain a decision advantage over a broad spectrum of hacktivists and other adversaries.

Want to learn more about the hacktivist DDoS landscape in Europe? Watch our Flash Talk on Turkish Hacktivism here.

Flashpoint Analyst Team

The Flashpoint analyst team is composed of subject-matter experts with tradecraft skills honed through years of operating in the most austere online environments, training in elite government and corporate environments, and building and leading intelligence programs across all sectors. Our team covers more than 20 languages including Arabic, Mandarin, Farsi, Turkish, Kazakh, Spanish, French, German, Russian, Ukrainian, Italian, and Portuguese.