Cytegic Special Intelligence Report - Belgium Terror Attack

March 23rd 2016

info@cytegic.com

cytegic

Cytegic Special Intelligence Update - Belgium Terror Attack

Following the terror attacks in Brussels on March 22nd, done by ISIS-affiliated terrorists, there is a heightened threat level in Belgium and Western Europe on the cyber front as well. Belgium is forecasted to experience cyber-attacks against high-profile websites and targets such as government and media.

We have been able to identify a pattern of behavior of cyber attackers and attack methods surrounding major terrorist events in Western Europe, the latest such pattern was identified after the November 2015 Paris terrorist attacks. This includes:

- The heightened cyber activity level in the attacked country starts directly after the terrorist attack and peaks during the week after, subsiding only two to three weeks later
- The most active cyber attackers are political activists (such as Anonymous and its affiliates), political cyber-warriors (nation-states or nation-backed attackers) and cyber-terrorists (usually hackers affiliating themselves with ISIS)
- The most used attack methods are denial-of-service, defacements, email social engineering and malware injections
- The most targeted industries in the attacked country are government, media, banking and finance, critical infrastructure, military and defense

After the Paris attacks, the cyber-war included two sides - French government forces, Anonymous and its affiliated on one side, and pro-ISIS hacktivists and sensationalists on the other. The cyber-skirmishes between the sides lasted for 3 weeks, peaking three and four days after the terrorist attack.

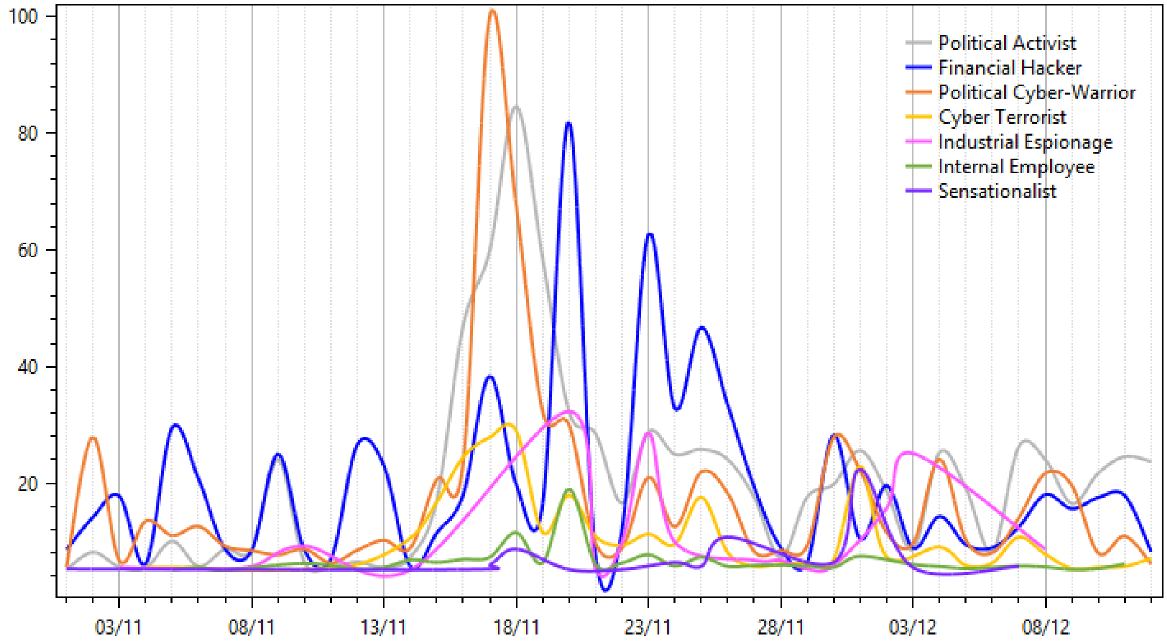
We have already been able to see political activists starting to “rally the troops” and organize for an anti-ISIS campaign, a continuation of the #OpISIS campaign. This usually includes attacks on ISIS supporting websites and social-media accounts - mostly denial-of-service attacks, defacements, website redirections and taking down twitter accounts. Previous attack methods also included dedicated attacks on ISIS related websites and users in order to dump data related mostly to recruiting.

It is important to mention the recent cyber-attacks on Ukrainian critical infrastructure and transportation targets, including Kiev’s international airport, a local railway company and an energy company, supposedly done by Russian government-backed hackers. These attacks are a foreseers of the upcoming cyber threat landscape, where hackers target critical infrastructure in order to cause chaos and physical damage, alongside fear and financial damage. Cyber terrorists are constantly looking to place “doomsday buttons” in critical infrastructure targets, and are more likely to continue doing so as the war against ISIS continues and grows.

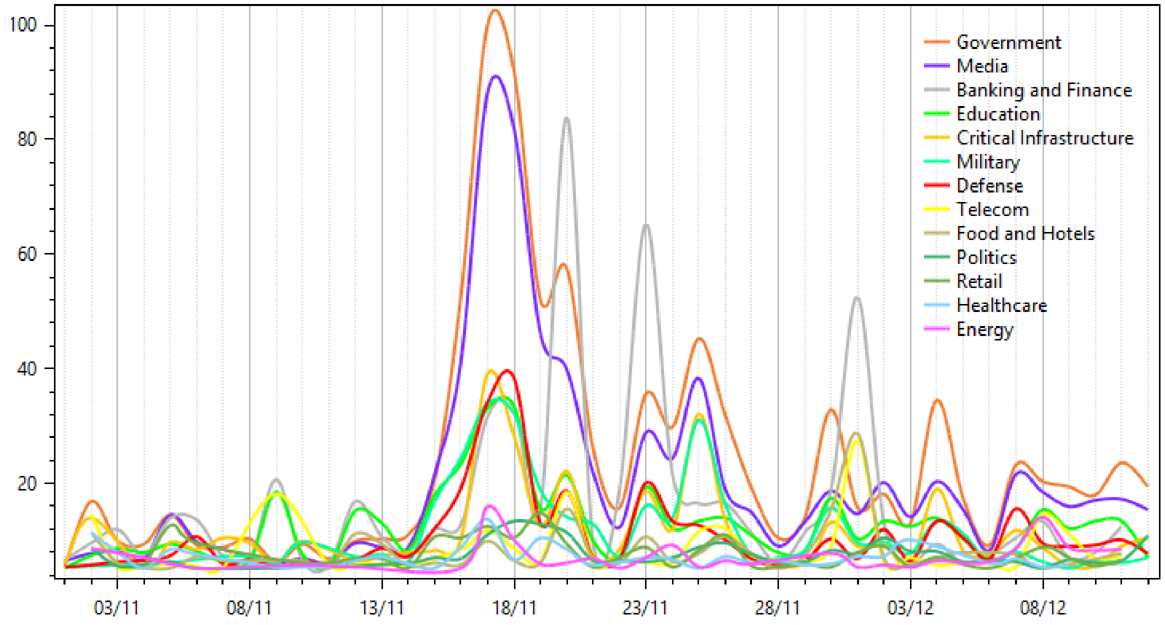
To conclude, high-profile organizations in Belgium and Western Europe, mainly from the government, media, banking and defense sectors should be on high alert for cyber-attacks in the coming weeks and take preemptive measures to prevent mostly DDOS, social-engineering and malware attacks on their websites, networks and employees.

Appendix - Infographics

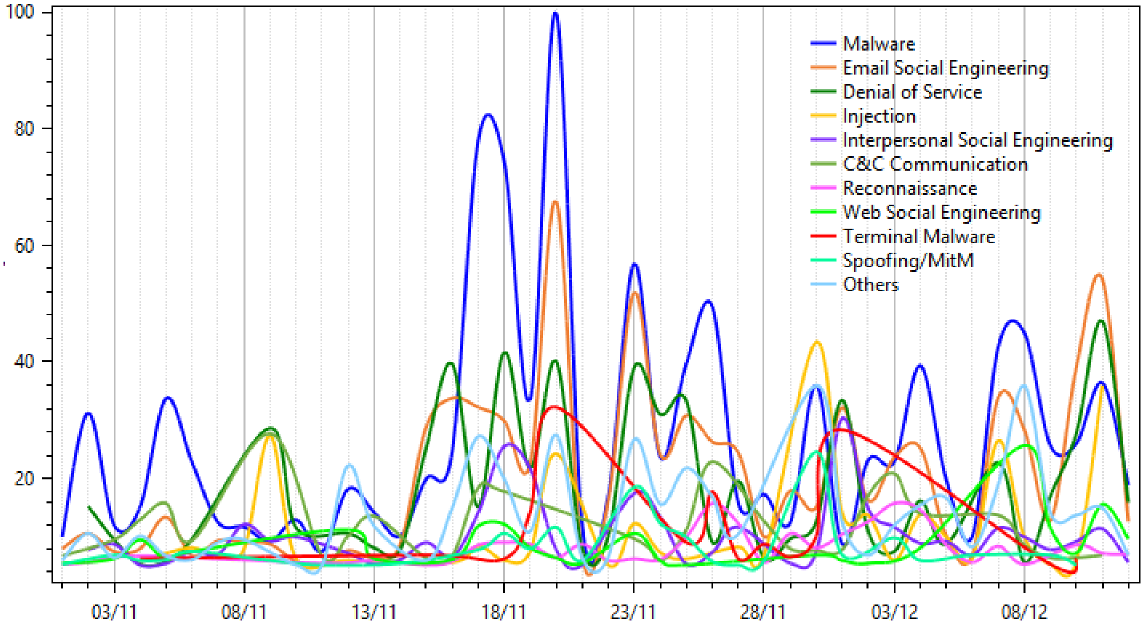
Paris attacks – top cyber attackers



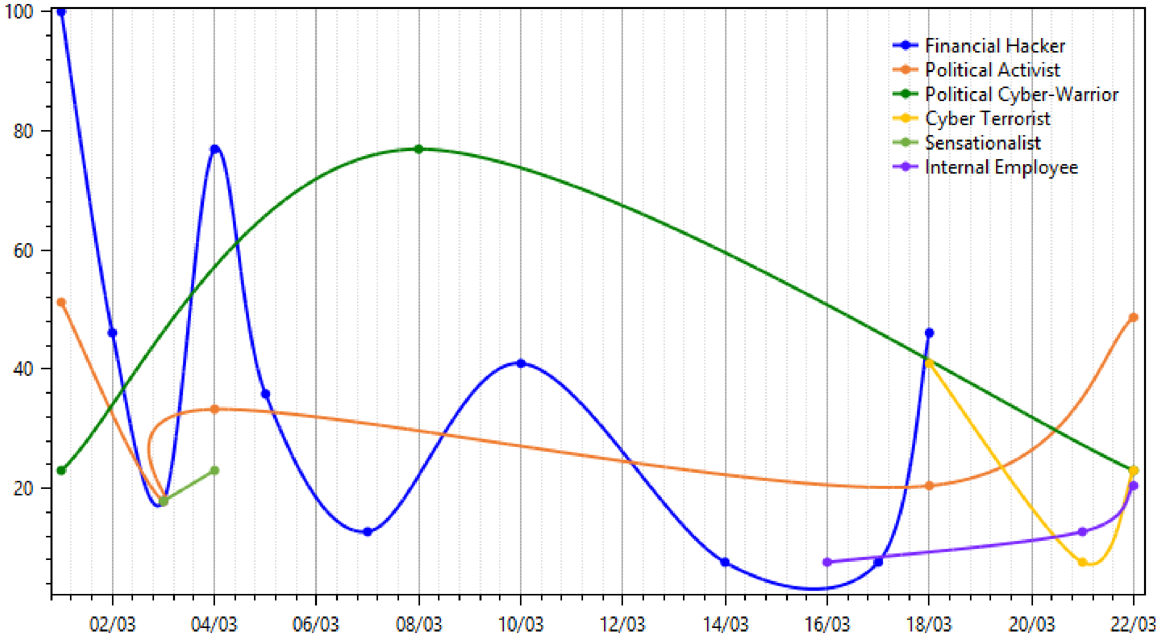
Paris attacks – most targeted industries



Paris attacks – most used attack methods



Belgium – Current attacker activity



About

This document was produced using the Cytegic DyTA intelligence platform.

Cytegic DyTA gathers, processes and analyzes hundreds of thousands of intelligence feeds from multiple sources on a monthly basis, to allow a quick and understandable cyber-trend analysis. DyTA enables cyber-intelligence analysts and CISOs to understand and analyze the threat level of each attacker and attack method relevant to their organization, according to their geo-political region, industry sector and corporate assets.

For further information please contact Cytegic at: info@cytegic.com