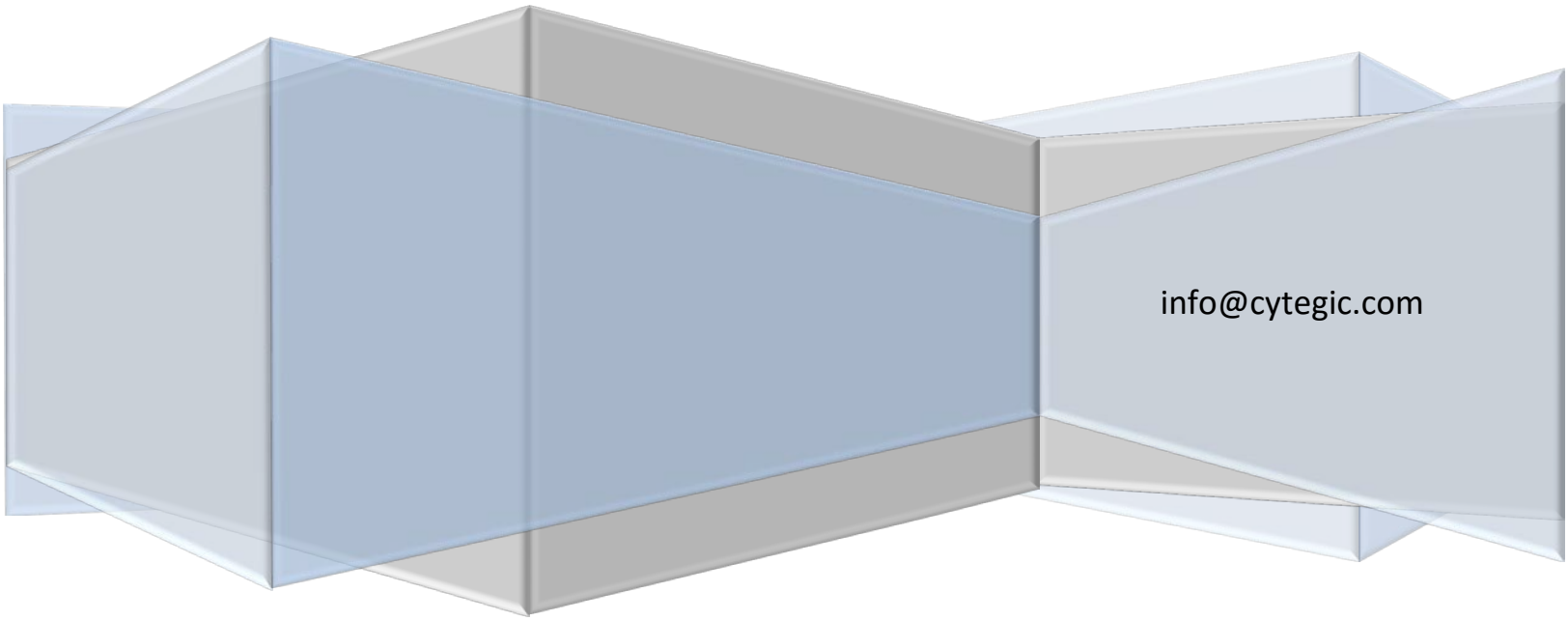
Cytegic Intelligence Report

November 2015



info@cytegic.com

Cytegic Intelligence Update

Background

The following intelligence report was generated using the Cytegic DyTA intelligence platform. The report represents the most interesting and note-worthy cyber-trends that were identified using DyTA.

Executive Summary

In November, Cytegic's DyTA processed and analyzed hundreds of thousands of data points from multiple sources and was able to identify, among others, the following trends and patterns:

- Unlike last month, Western Europe surpassed North America as the most targeted and cyber-active geo-political region in the world, attributed in part to the Paris terrorist attacks and their consequences.

- The UK and Syria continued to be the most targeted countries in Western Europe and the Middle-East, respectively. But, France experienced a high jump, taking second place in Western Europe after a long period trailing after Germany, and Iraq and Turkey also became much more active, partially due to tensions surrounding military operations.

- An analysis of the weeks before and after Thanksgiving shows that the pattern we observed in previous holidays (as Halloween) and have forecasted for the holiday season repeated itself, when the week before Thanksgiving witnessing a dramatic rise in Malware and specifically Point of Sale Malware attacks on retailers. Also, it is interesting to see that the most used attack method during Cyber Monday was Email Social Engineering, which coincides with the behavior of retailers and online shoppers. These patterns and trend will continue throughout December and peak in the weeks before Christmas.

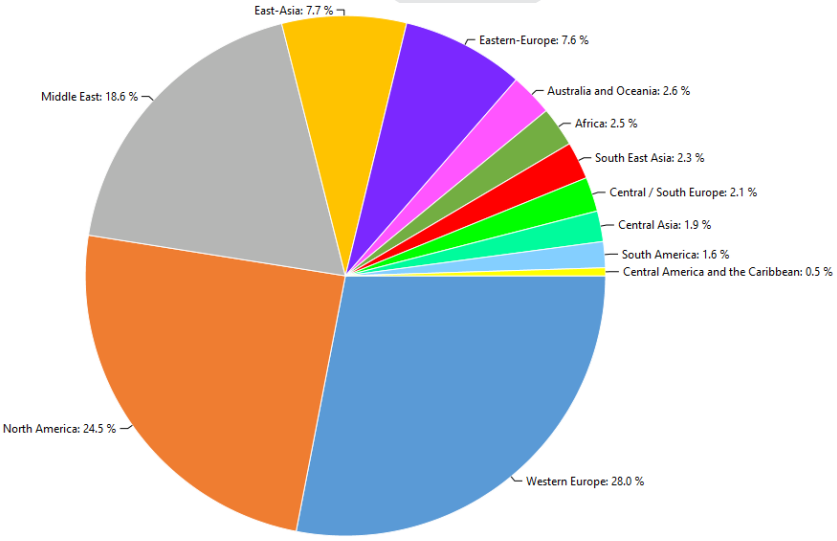
- As in last month's report, an interesting comparison analysis between Cytegic's open-source intelligence and Sixgill's Darkweb intelligence sheds some light on the most sought-after assets in North America. As we forecasted, Payment Card details have risen the become the second most targeted asset, after Client Data, due to the holiday season in North America (surpassing Monetary Value and Financial Transactions)

- Last but not least, an analysis of the cyber-consequences of the November 13th Paris terrorist attacks, reveals that in the weeks before the attacks there was hardly any cyber-terrorist activity, and it focused mostly on Government, Critical Infrastructure and Military targets ("the usual targets"). But, right before the attacks, and much more significantly in the days after the attacks, the cyber-terrorist activity rose dramatically against a wide array of industries, subsiding only after two weeks

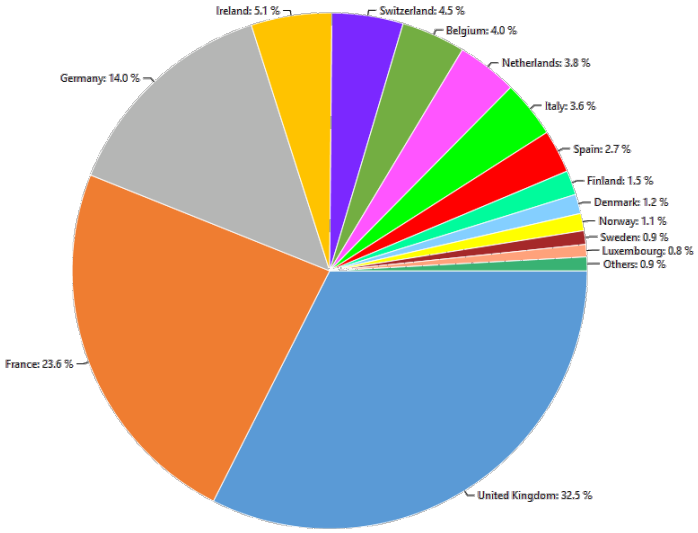
Top Trends:

Most Active Geo-Political Regions

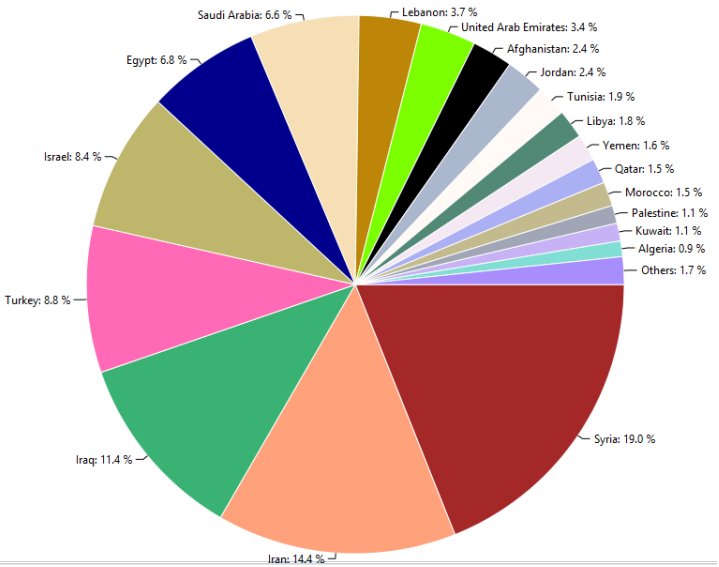
In November 2015, the most cyber-active geo-political regions, analyzed using the DyTA platform, were Western-Europe, North America and the Middle East, with Western Europe surpassing North America for the first time in months, partly due to the terrorist attacks in France and their aftermath throughout Europe



In Western Europe the most active country was the UK, continuing the trend from previous months, but this month France took second-place due to the aforementioned terrorist attacks and the cyber war between ISIS-supporters and affiliates on one side and the French government and Anonymous on the other



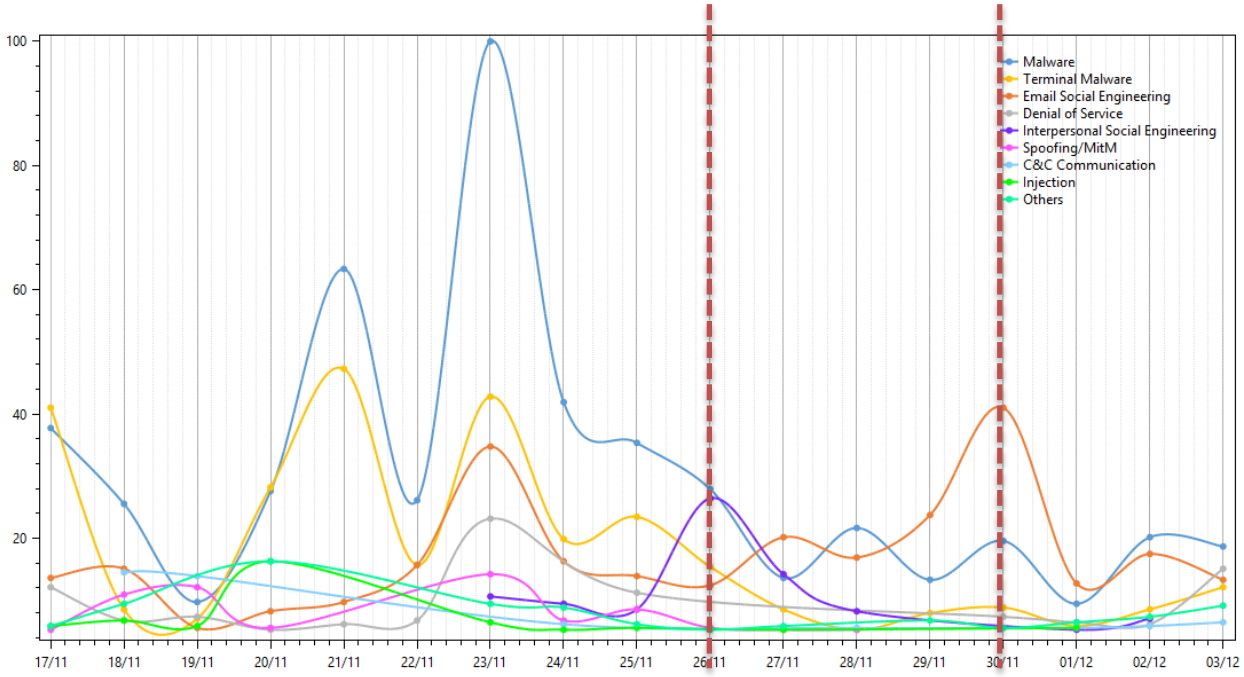
In the Middle East, Syria continues to be the most cyber-active country, followed by Iran. This month Israel was pushed aside a bit, giving way for Iraq and Turkey as runner-ups. This could be attributed in part to the rising tensions between Turkey and Russia, and Turkey and Iraq over military operations in Syria and Kurdistan (respectively)



Top Attack Methods Used Against Retailers in North America Surrounding Thanksgiving

Following our analysis in last month's report about Halloween as a foreseer of the holiday season, this month we analyzed the attack methods used against retailers in North America in the week before and after Thanksgiving weekend. As we predicted, the week before Thanksgiving saw a significant rise in attacks, mostly of Malware and Terminal Malware (especially Point of Sale), which coincides with the behaviors of shoppers in stores. While attacks subsided somewhat during the weekend itself, we can see a sharp rise in Email Social Engineering during Cyber Monday. This fits the pattern of email scams during Cyber Monday from previous years, when financial hackers take advantage of the email blasts from retailers in order to attack them and their clients, during that special sales day.

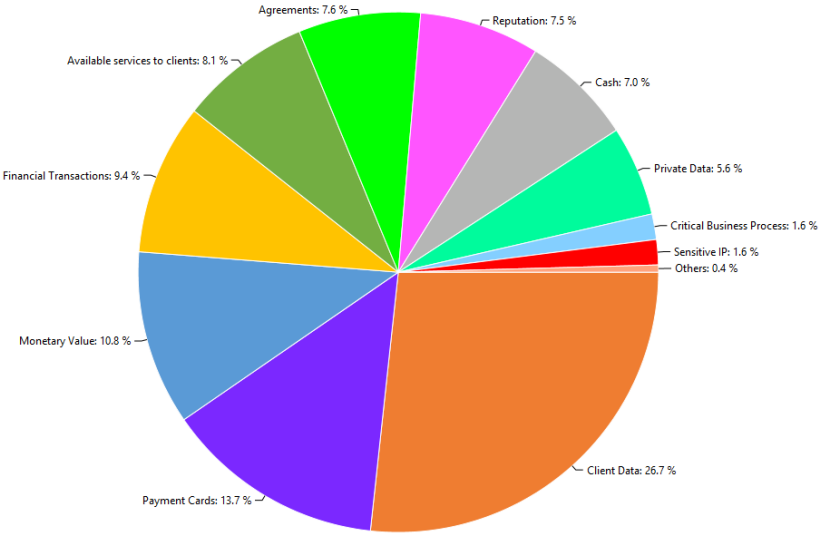
We forecast these patterns and trend continuing during December, peaking before Christmas and New Year's.



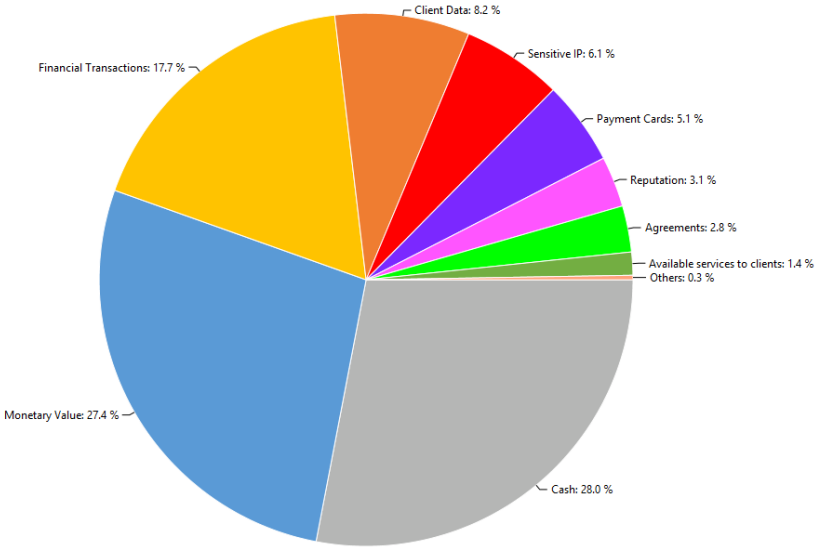
Most Targeted Assets in North America

When examining the most targeted assets it is interesting to compare between Cytegic's Open-Source intelligence feed and the Darkweb intelligence feed from our friends at Sixgill. As we forecasted, Payment Card details have risen the become the second most targeted asset, after Client Data, due to the holiday season in North America (surpassing Monetary Value and Financial Transactions). But, it is still less prominent in Darkweb forums, suggesting that either this year's attacks were less successful or that the attackers haven't put these credentials for sale yet. Thus, Cash, Monetary Value (mainly Bank Accounts), Financial Transactions and Client Data remain as the most active assets on the Darkweb.

Cytegic's Open-Source Intelligence



Sixgill's Darkweb Intelligence

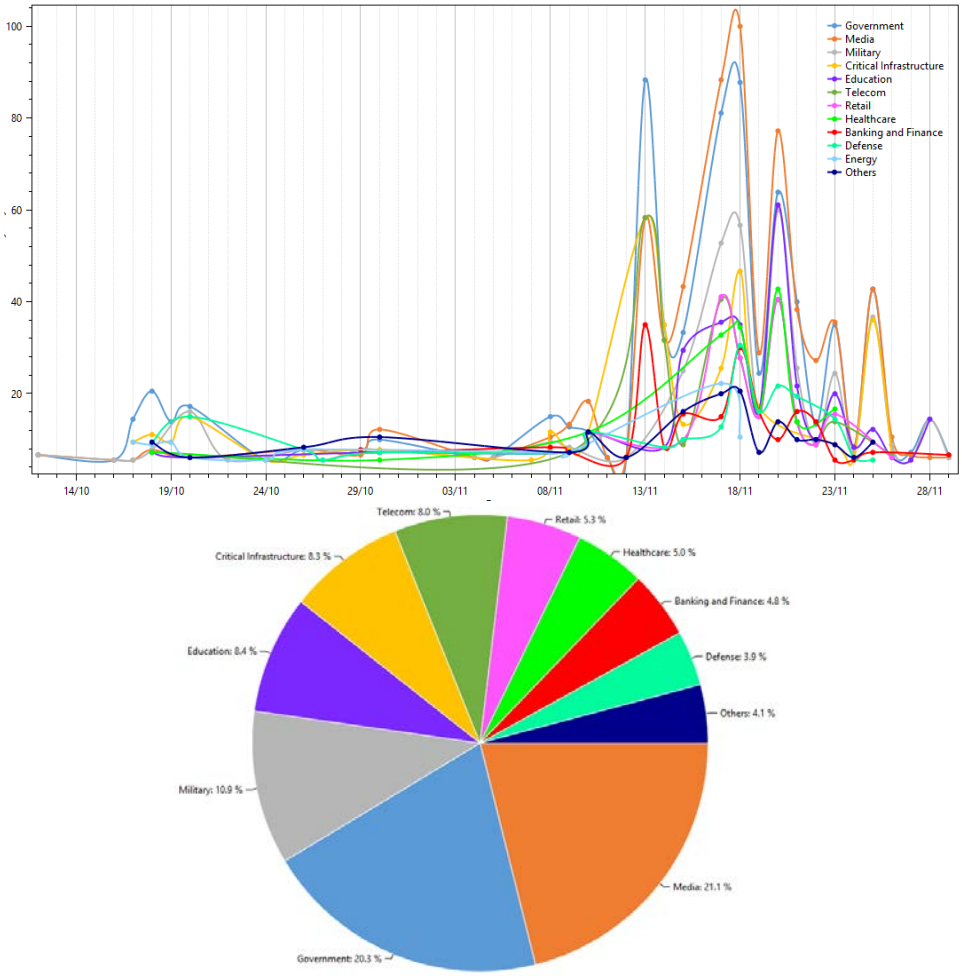


The Impact of the Paris Terrorist Attacks on the European and North American Threat Landscape

On November 13th Paris, France experienced its severest terrorist attack in history, done by ISIS members and affiliates. The attack triggered a "cyber-war" between ISIS-affiliated hackers and the Anonymous Collective. Skirmishes like these occur almost regularly after a major terrorist attack between the two sides (as seen after previous attacks in France, Belgium and Denmark).

Below is a graph showing the activity of Cyber-Terrorists, in Western Europe and North America, in the weeks before and after the Paris attacks (by Industries). It is interesting to note that in the weeks before the attacks there was hardly any cyber-terrorist activity, and it focused mostly on Government, Critical Infrastructure and Military targets ("the usual targets"). But, right before the attacks, and much more significantly in the days after the attacks, the cyber-terrorist activity rose dramatically against a wide array of industries, subsiding only after two weeks. In this period the most targeted industries were Media, Government and Military, but other industries such as Education, Telecom and Banking and Finance also received ricochets from the conflict.

These insights have actionable implications on cybersecurity management and resource allocation. Cybersecurity professionals should take note of these patterns and be aware and prepared for the attacks that will follow the unfortunately-inevitable next terrorist attack in the Western world.



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