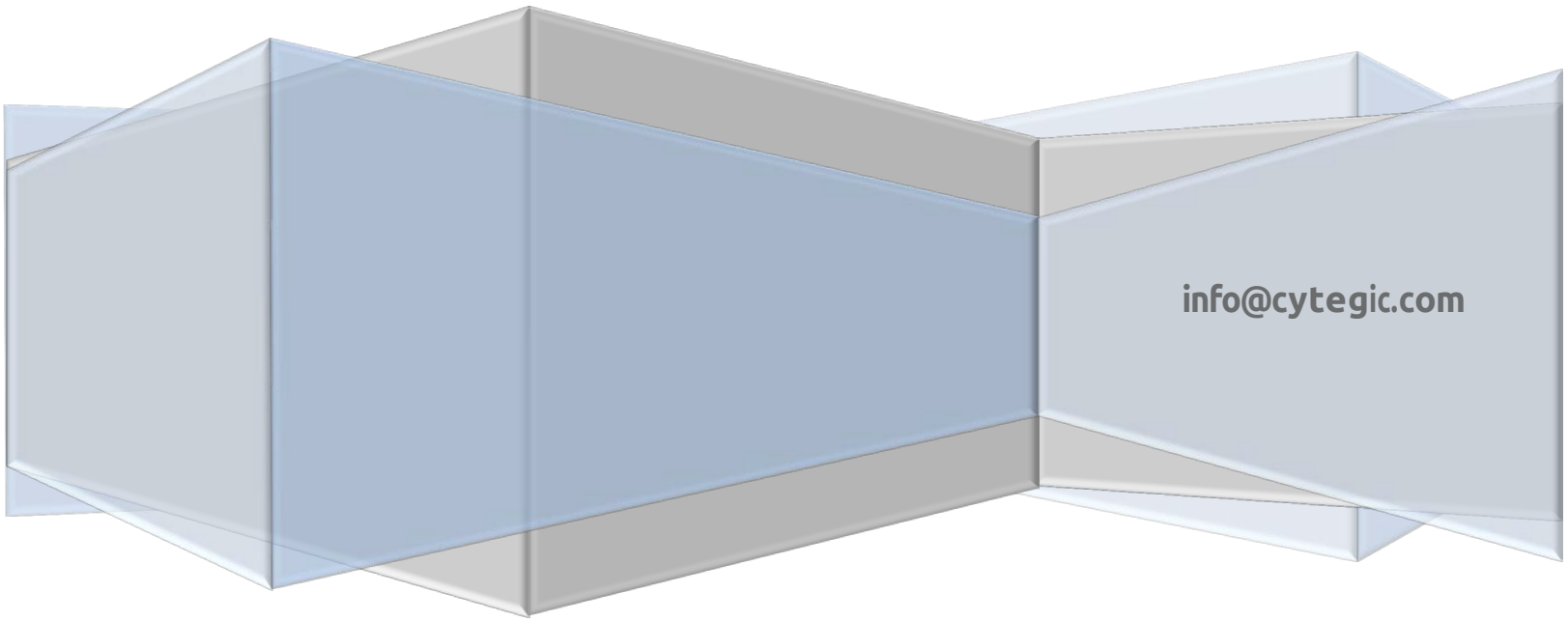
cytegic

DyTA Intelligence Update

February 2015



info@cytegic.com

February 2015 - Cytegic DyTA Monthly Intelligence Update

Intro

Cytegic DyTA intelligence platform gathers, processes and analyses hundreds of thousands of intelligence feeds on a month 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.

The following report represents the most interesting and active cyber-trends that DyTA analyzed, in addition to noteworthy vulnerabilities, malware developments and cyber-attacks and campaigns.

Executive Summary

Interesting trends:

- In North America, the most active attackers were financial hackers and politically-motivated attackers (nation-states, hacktivists, etc.). But, while the volatility of financial attackers was high, we could see that political cyber-warriors, mainly conducting cyber-espionage, were much steadier.
- The most targeted asset in North America was client data, used mostly to commit fraud, accounting for 35% of the targeted assets. More “traditional” financial assets, such as agreements, transactions and payment cards also accounted for almost 30%.

Noteworthy attacks and campaigns:

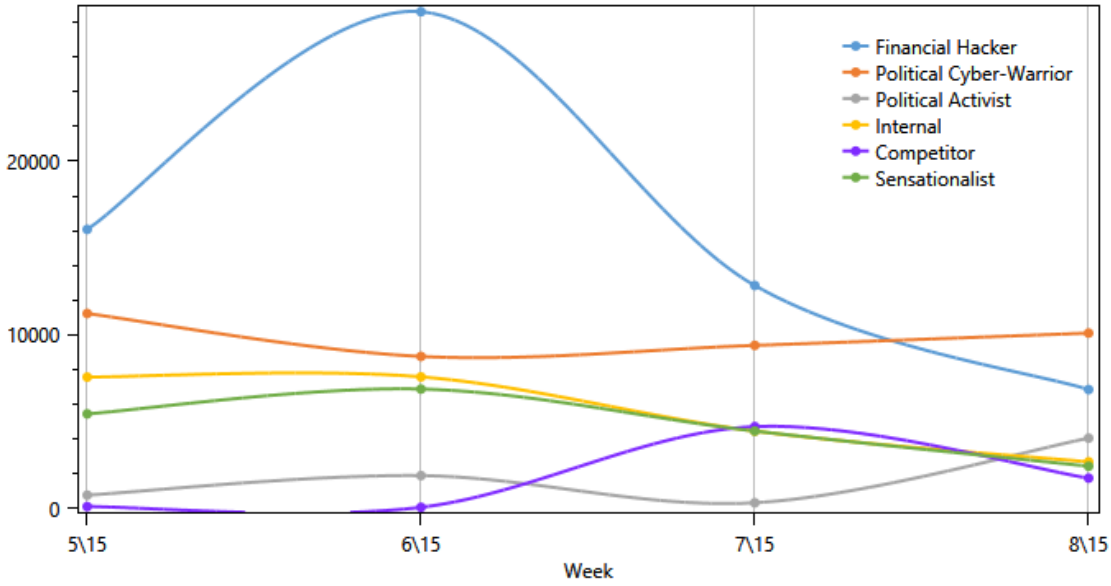
- American insurance giant Anthem has been breached, and up to 80 million of its customers have had their Social Security Numbers and other sensitive data stolen
- Several very interesting cyber-espionage campaigns and groups have been uncovered - Middle-Eastern Arid Viper campaign and Desert Falcons group; Operation Pawn Storm which targeted iOS devices of high-ranking government personnel; the hacking of Gemalto’s SIM cards; and Equation Group, an advanced nation-state espionage actor, which has been active for almost 20 years
- Eastern European hackers, nicknamed the Carbanak ring, managed to steal up to 1 billion dollars from over 100 banks worldwide

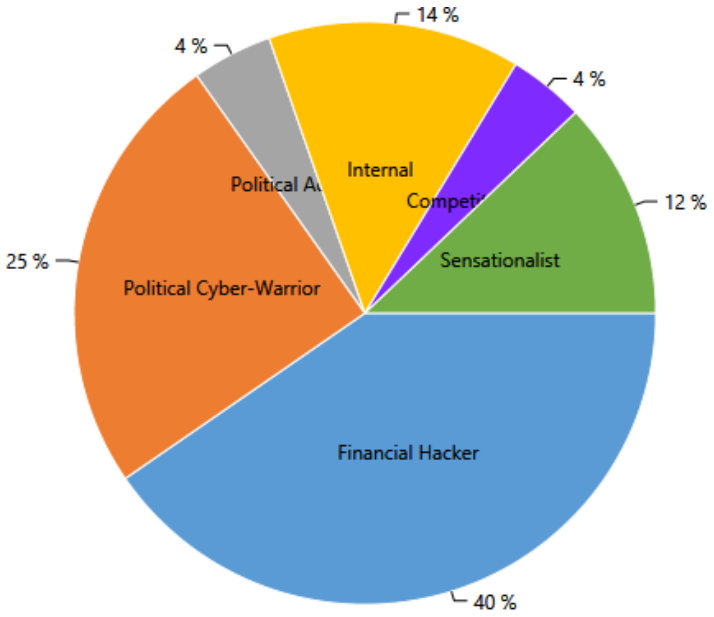
info@cytegic.com

Top trends

a. North-America Top Attackers

In the past month, financial hackers continued to be the most active and threatening attackers in North-America, making for 40% of the cyber-attacks, though their threat level fluctuates often. The activity level of Political Cyber-warriors (nation-states, terrorists and espionage groups), on the other hand, remained at a steady level throughout the month. This coincides with our assessments - national cyber-espionage (with APTs as part of it) is by nature less volatile and less prone to changes than financially or sensation-motivated attacks.



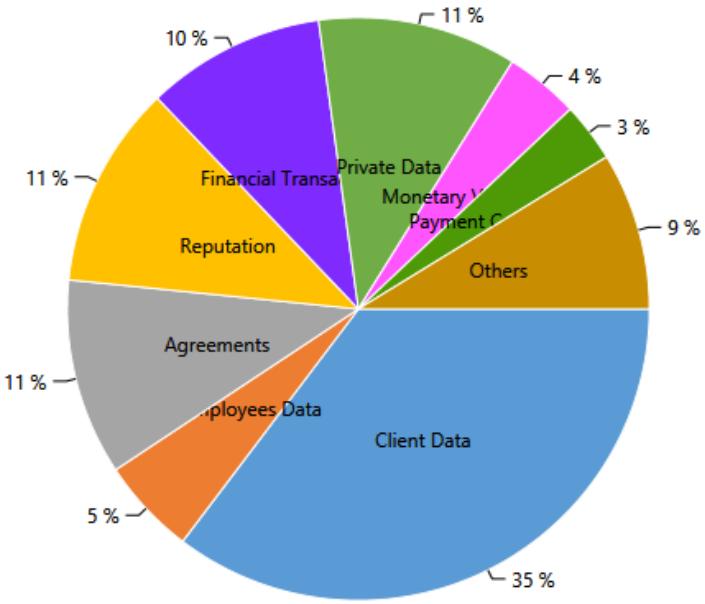


b. North-America Most Targeted Assets

Client Data, consisting, amongst others, of personally identifiable information (PII) and customer IDs and passwords, has been the most sought-after asset in North-America this month, making for 35% of the most targeted assets in the region. More "obvious" financial assets, such as agreements, transactions and payment cards also accounted for almost 30%.

These statistics emphasize two of the top trends we discussed in previous updates and in our 2015 forecast -

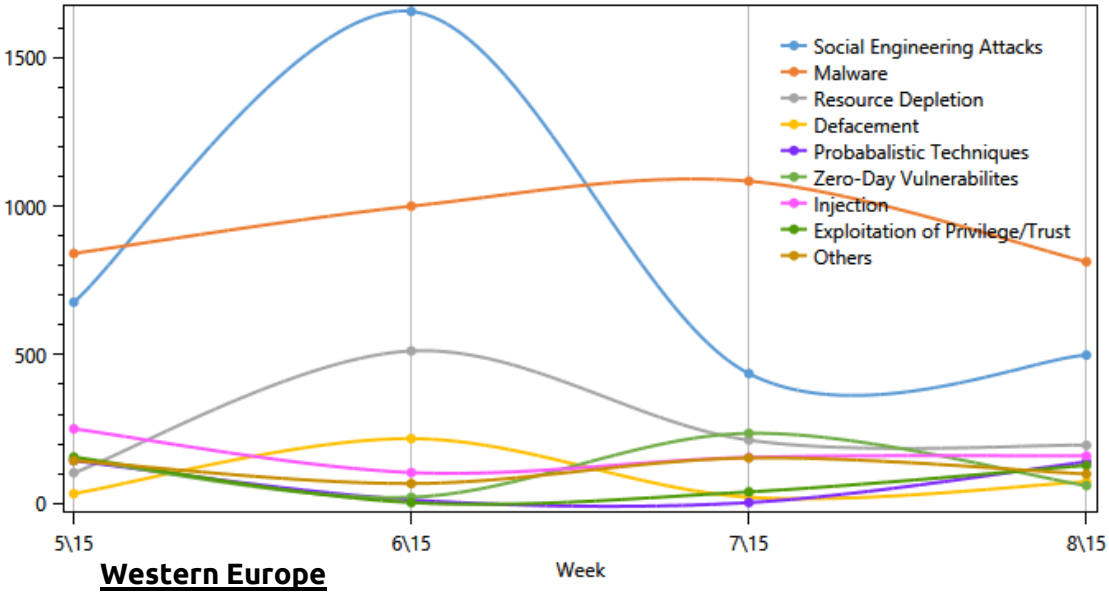
- PII remains very attractive for financially motivated hackers, which use the information to commit fraud (such as banking fraud) or sell it on online black markets.
- While POS malware, used to steal payment-card details, gained many headlines during the previous months, its activity level declined after the beginning of the year. This type of attack usually coincides with shopping seasons, and now that the holiday season is over, the activity level returned to its "natural state".



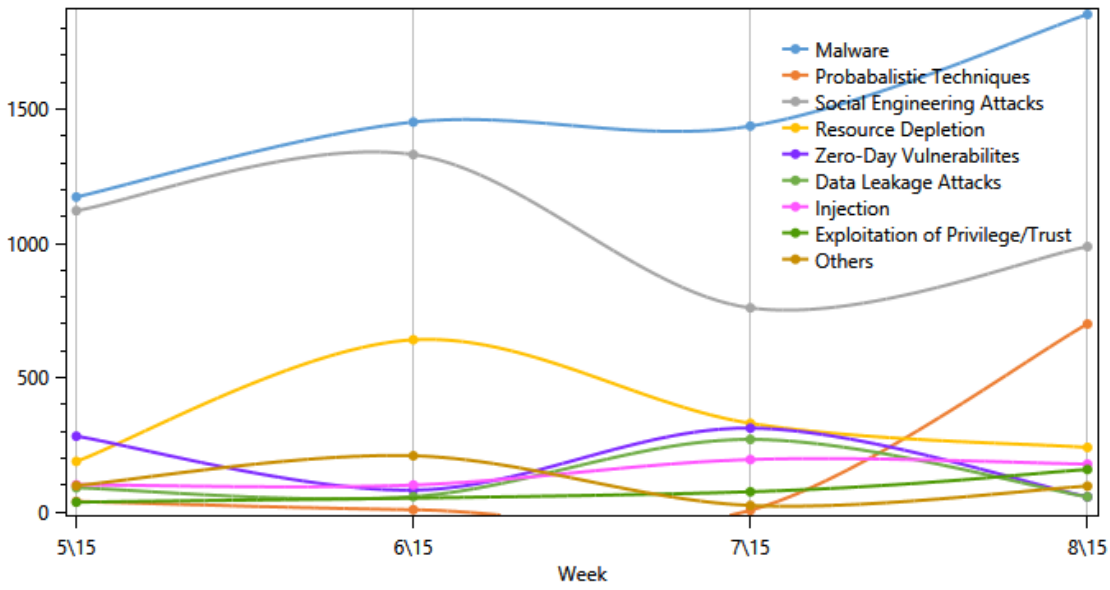
c. Banking and Finance Sector - North America vs. Western Europe - top TTPs

DyTA enables analysts to conduct cross-sector and cross-GeoPol research and analysis. As such, when comparing the TTPs targeting the financial sectors in North America and Western Europe several interesting insights appear. For once, malware and social-engineering attacks dominated both areas in the past month. But, while North-America has seen a slight decline in the activity level of these attacks, Western Europe's threat level rose systematically throughout the month. Additionally, the other top TTPs "behave" quite similarly, meaning the threat to the sector is similar across continents.

North America



Western Europe



Main Incidents, Alerts and Developments

1. **Anthem Breach**[1] - Earlier this month it was reported that American insurance giant Anthem has been breached, and up to 80 million of its customers have had their Social Security Numbers and other sensitive data stolen. The reports are pointing the finger at nation-backed attackers from China. According to the publication in Bloomberg[2], the attacks seem to be part of an espionage campaign aimed at stealing medical data in order to spy on American government and defense personnel. The breach also affected up to 18 million non-Anthem customers.

   The consequences of such attacks are devastating to large companies. As an example, it was reported this month that the cost of the 2013 Target breach cost the company some 160 million dollars. And another noteworthy consequence - Amy Pascal, co-chair of Sony Pictures Entertainment and chair of Sony's motion pictures group, will step down in May from her executive posts
2. **Cyber-Espionage** - This month, several very interesting cyber-espionage campaigns and groups have been uncovered (partially because Kaspersky waited for their annual Analyst Summit to publish their researches). Among these were the Middle-Eastern Arid Viper campaign and Desert Falcons group, the first high-end Arabic-based cyber-espionage campaigns; Operation Pawn Storm[3] which targeted iOS devices of high-ranking government personnel; and the hacking of Gemalto's SIM cards[4], apparently conducted by the NSA and/or GCHQ, which lasted for years before being uncovered this month.

   Above all, there is the publication regarding the so-called Equation Group[5]. The group has been active, in one form or another, for almost 20 years and, according to Kaspersky's research, conducted long-lasting, highly affective, highly sophisticated, stealth malware campaigns globally against military, government, telecom, energy and more sectors. The group developed dedicated malware, worms and even two modules which allow reprogramming of the hard-drive firmware. The sophistication and persistence levels suggest that the group is part of a Western nation-state effort.

[1] http://news.softpedia.com/news/Up-to-18-8-Million-Non-Anthem-Customers-Affected-By-the-Data-Breach-474265.shtml
[2] http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack
[3] http://www.scmagazine.com/spyware-apps-are-targeting-high-profile-government-personnel/article/396488/
[4] http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx
[5] http://www.net-security.org/malware_news.php?id=2966

3. **Financial Hackers steal hundreds of millions of dollars from banks**[6] **-** Eastern European hackers, nicknamed the Carbanak ring, managed to steal up to 1 billion dollars from over 100 banks worldwide. The organized crime ring managed to do so by targeting specific personnel in the banks with spear-phishing techniques, inject their systems with the Carbanak trojan and then navigate in the banks' systems until reaching their goal. The attackers were able to take control of victimized computers and networks and use them in order to transfer money to specific accounts and make ATMs to dispense cash on command. This is part of a global, steady trend of money-stealing malware attacks, which is usually conducted by Russian and Eastern European groups.
4. **Hacktivists vs. Terrorists** - Last month, we reported about the rise in the "cyber-war" between ISIS-supporters and Hacktivists, mostly Anonymous-related. This is part of a consistent trend which has seen a sharp rise after the terror attacks in France.
    a. OpISIS - This month, Anonymous continued they OpISIS campaign, taking down more than 1000 ISIS-related websites, and dozens of social-media accounts. The attacks consisted mostly of DDoS techniques, as Anonymous is used to do. The Hacktivist collective released a video stating they will continue their campaign as long as ISIS exists.
    b. Cyber Caliphate Takes Over Newsweek - Cyber Caliphate, the high-profile ISIS-affiliated hackers, on their end, were able to hijack Newsweek's Twitter account. The hackers took control of the account and posted several tweets against President Obama, and the US government. This is a continuation of the attacks conducted by Cyber Caliphate against the US from last month.

[6] http://threatpost.com/carbanak-ring-steals-1-billion-from-banks/111054