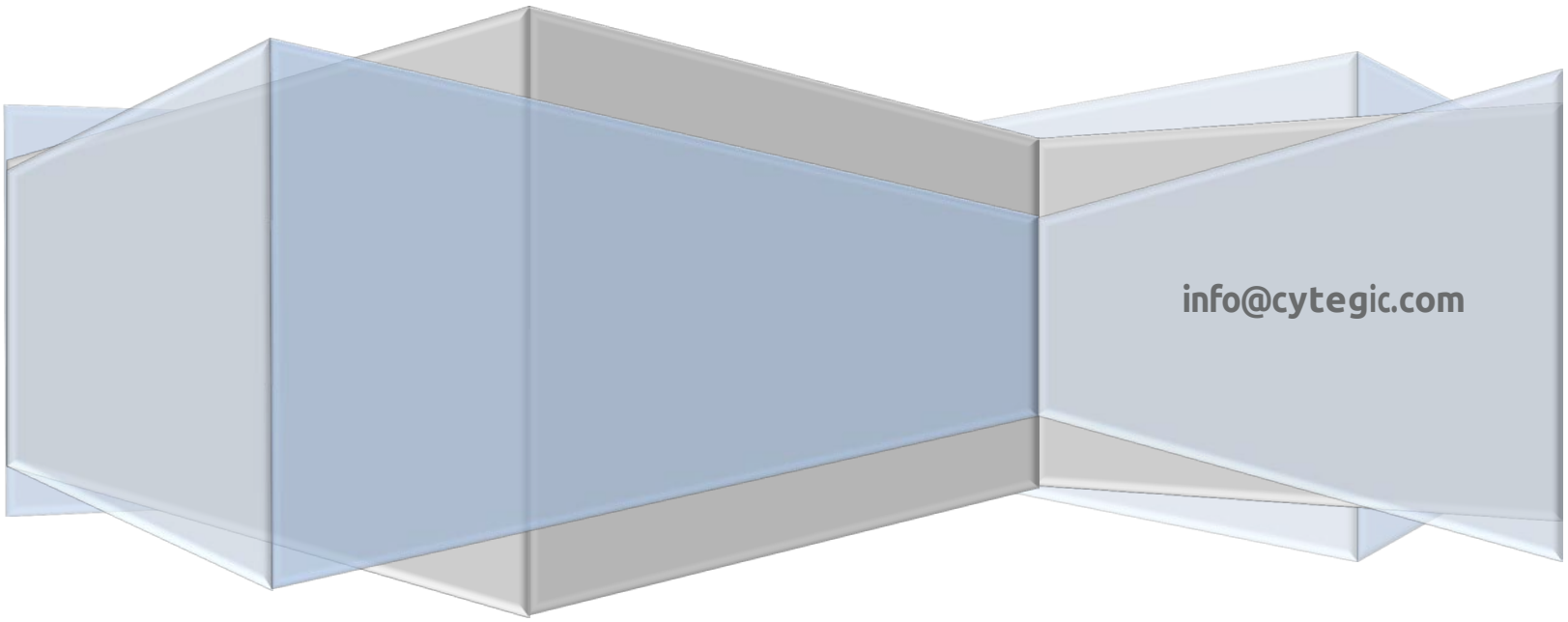
cytegic

DyTA Intelligence Update

March 2015



info@cytegic.com

March 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:

- The FREAK vulnerability - the SSL/TLS vulnerability which allows for Man-in-the-Middle attacks was published this month, causing a large spike in attack in the beginning of the month. The most interesting pattern that appeared from the behavior analysis was that the publication affected most types of attack methods and not only MitM. This can be attributed to attackers taking advantage of the "panic" and shift in security teams' focus in order to perform attacks other than those enabled directly by the vulnerability.
- As in last month, the most targeted asset in North America was client data, as in the Premera breach, accounting for 47% of the targeted assets (a significant increase). It is interesting the see that it is also a global trend, with client data amounting to 53% around the world.

Noteworthy attacks and campaigns:

- Another American insurance giant hacked - 11 million of Premera Blue Cross customers affected by the breach
- A new and highly-sophisticated Point-of-Sale malware has been discovered named PoSeidon. It appears to be the most sophisticated PoS malware yet and it shares many of its characteristics with the infamous Zeus banking trojan

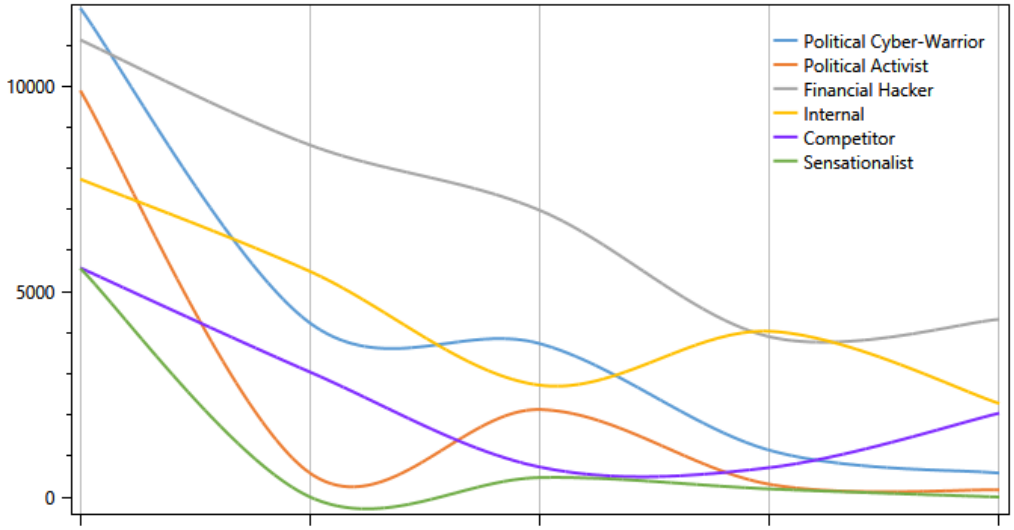
info@cytegic.com

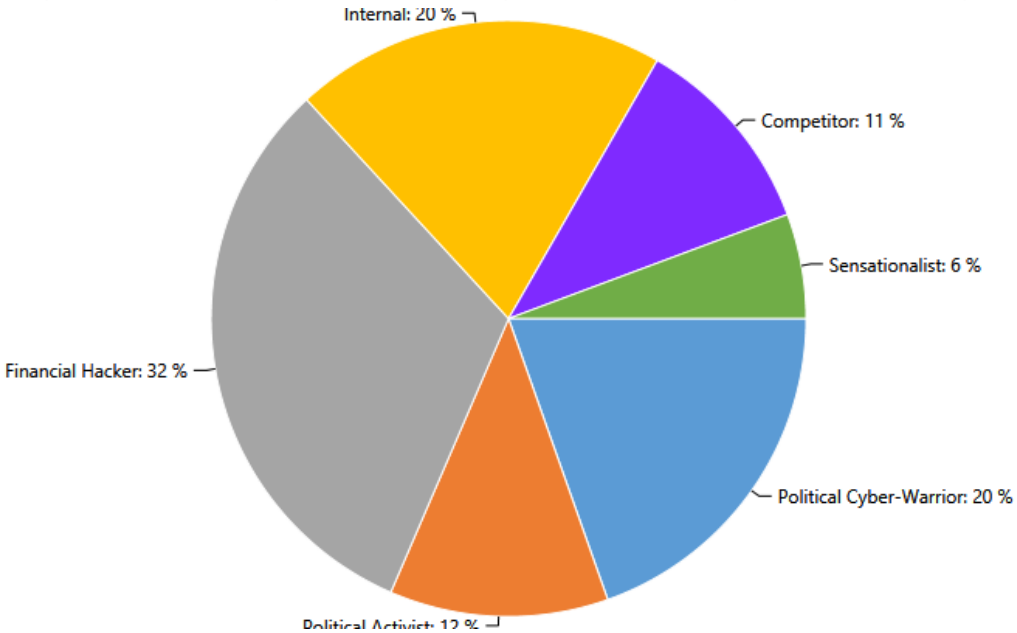
Top trends

a. North-America Top Attackers

In the beginning of March we have seen a sharp spike in activity level for all of the attackers. This can be explained by the publication of the FREAK vulnerability, which stirred the cyber world, but very quickly subsided. After the storm has passed (or has it?) the activity levels of most attackers returned to “normal”, with financial hackers and political cyber-warriors taking the lead.

Nevertheless there have been several interesting changes, including the rise in competitor, internal and political activist behavior, which took a bite of the pie from financial hackers and political cyber-warriors. The rise in competitor activity can be attributed to the FREAK MitM capability, and the rise in political activist can be attributed to the high-profile nuclear talks in Switzerland and the new war in Yemen (among others).

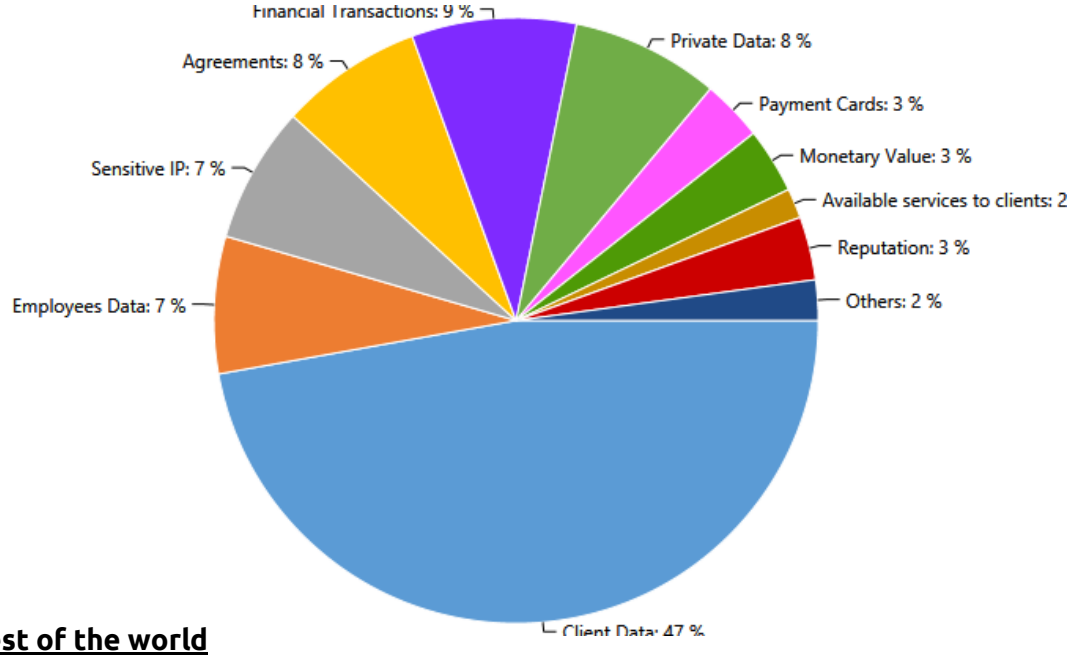




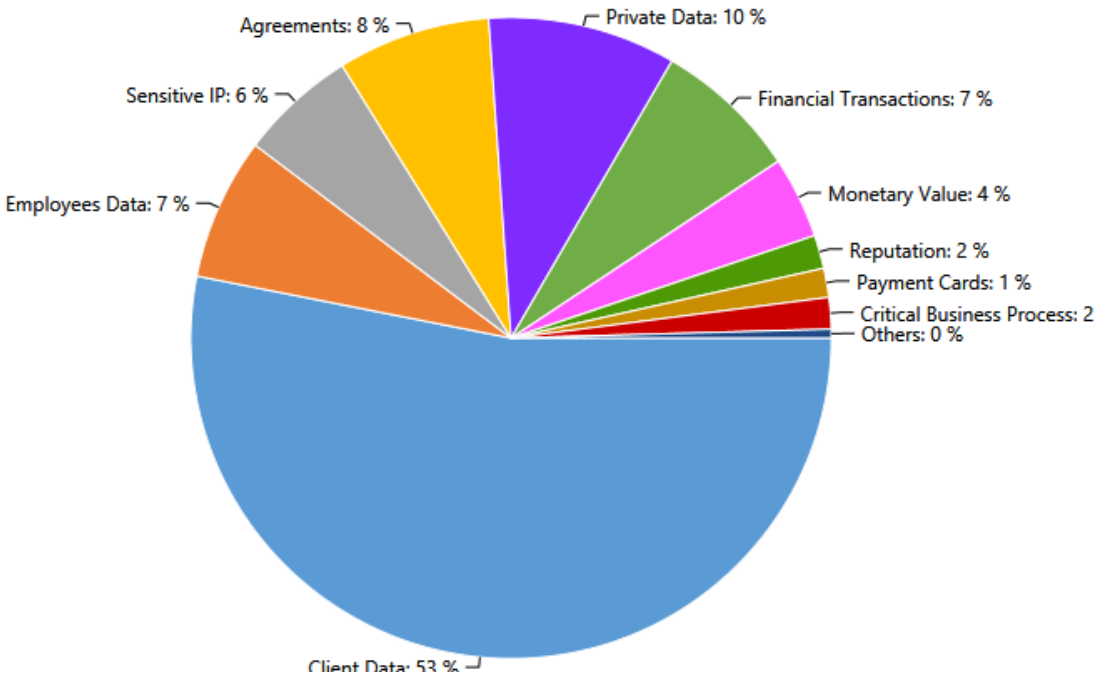
b. Most Targeted Assets

As in last month's update, Client Data, consisting, amongst others, of personally identifiable information (PII) and customer IDs and passwords, continued to dominate the "most wanted asset" list and in fact has risen from 35% to 38% in North America. This is due to the much discussed trend of rising monetization of PII and personal data in underground cyber-crime forums. When compared to the rest of the world, the trend is emphasized even more, making PII the "Most Valuable Asset" of 2015 Q1 globally.

North America



Rest of the world

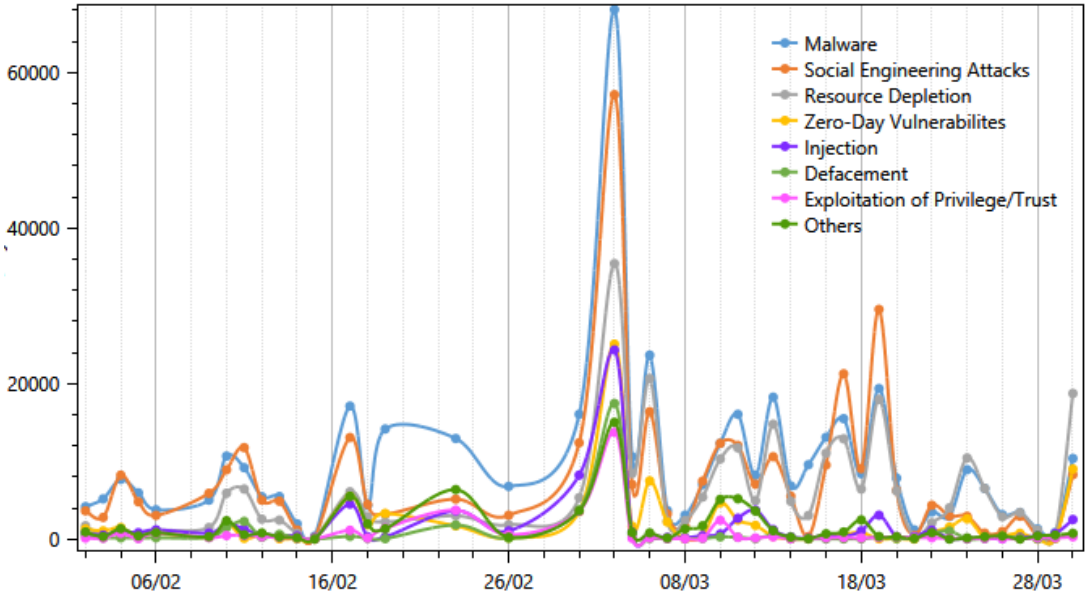


c. The FREAK Vulnerability

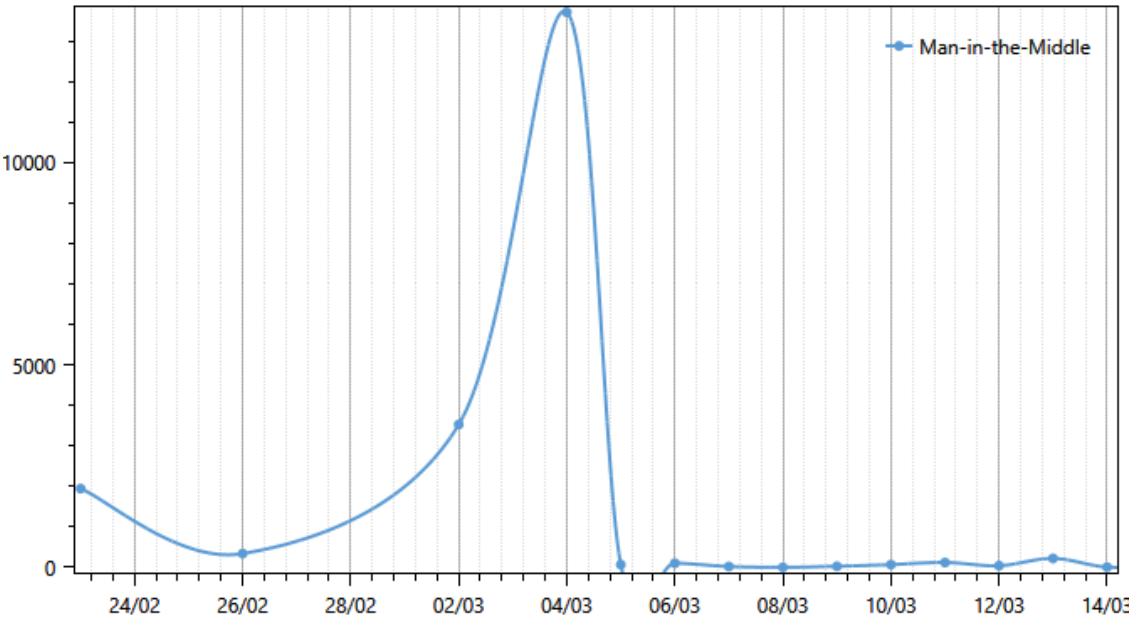
On March 3rd, a new and alarming TLS/SSL vulnerability was discovered - FREAK. The vulnerability allows for a "man in the middle" attack by tricking the user and the server into accepting a weak version of HTTPS encryption.

It is interesting to see the impact the vulnerability publication had on different attack methods, MitM included, and attacker behavior. The sudden spike in activity for most attack methods can be explained by claiming that attackers often chose to check their capabilities and take advantage of the panic and shift in focus of security teams during the publication of such major vulnerabilities. As such, security teams should be aware of this pattern and better allocate their defenses for future vulnerability publications, not only against the mentioned vulnerability.

Effect on all attack methods



Effect on MitM



Main Incidents, Alerts and Developments

1. **Premera Blue Cross breached**[1] - After last month's huge Anthem breach, Premera Blue Cross, another large American health insurance company also announced it was breached, exposing information of as many as 11 million of its customers. Both this and the Anthem attack were apparently done using similar methods, including fake websites for phishing and spoofed certificates, suggesting one attacker is behind both. Regardless of whom the specific attacker is, it is clear the PII and health records especially are a valuable target for hackers, and can be used to perform fraud, impersonations, financial theft and other financial crimes.
2. **New PoSeidon malware**[2] **-** A new and highly-sophisticated Point-of-Sale malware has been discovered named PoSeidon. According to the researchers at Cisco, who discovered the malware, it is the most sophisticated PoS malware yet and it shares many of its characteristics with the infamous Zeus banking trojan. The malware was built to be highly evasive, communicate directly with C&C servers and self-update for newer versions[3]. The malware not only scrapes the PoS memory for payment card details, but also checks if the cards are valid and even installs a keylogger to steal credentials.
3. **GitHub attacked by massive DDOS**[4] - The large code-sharing platform GitHub suffered the harshest DDoS attack is its history this month, which lasted for over a week. According to researchers, it appears that most of the traffic was directed from China, a large part of it directed from the Baidu search engine. Several speculations have been made regarding the reason behind the attacks, some suggesting it was done in order to block anti-censorship tools hosted on GitHub. A similar attack was conducted this month against the GreatFire activist group's website, which also confronts censorship in China.

[1] http://www.csoonline.com/article/2898111/business-continuity/premera-blue-cross-says-data-breach-may-affect-11-million-customers.html
[2] http://securityaffairs.co/wordpress/35181/cyber-crime/poseidon-pos-malware.html
[3] http://blogs.cisco.com/security/talos/poseidon
[4] http://www.securityweek.com/china-suspected-software-site-github-hit-attack