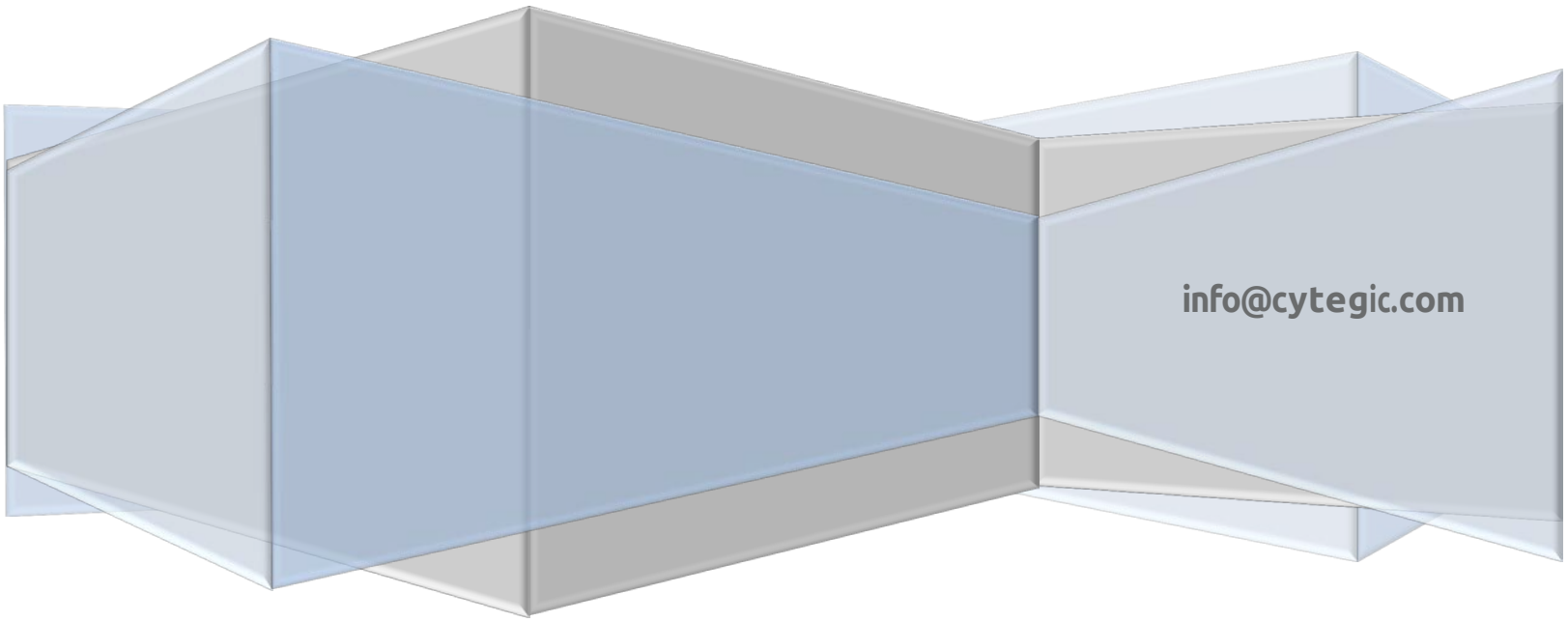
cytegic

DyTA Intelligence Update

April 2015



info@cytegic.com

April 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:

- April compared to March - In North America, attackers were significantly more active in April than in March. As our DyTA system forecasted, the rising trend began at the end of March and continued throughout April. The trend was especially dominant with financial hackers, political cyber-warriors (nation-states and terrorists) and the insider threat. According to our forecasts, this trend will continue to rise in the coming weeks.
- OpIsrael - while the annual hacktivist campaign against Israel was a dud, our DyTA system was able to identify several interesting patterns:
    - The attacks started to become severe a week before April 7th and in some cases lasted until, and even peaked, a week after.
    - The IT sector (ISPs included) was predominant, followed by media, banks and government. The attacks on the IT sector had a strengthening wave pattern, with a couple of days between each wave.

Noteworthy attacks and campaigns:

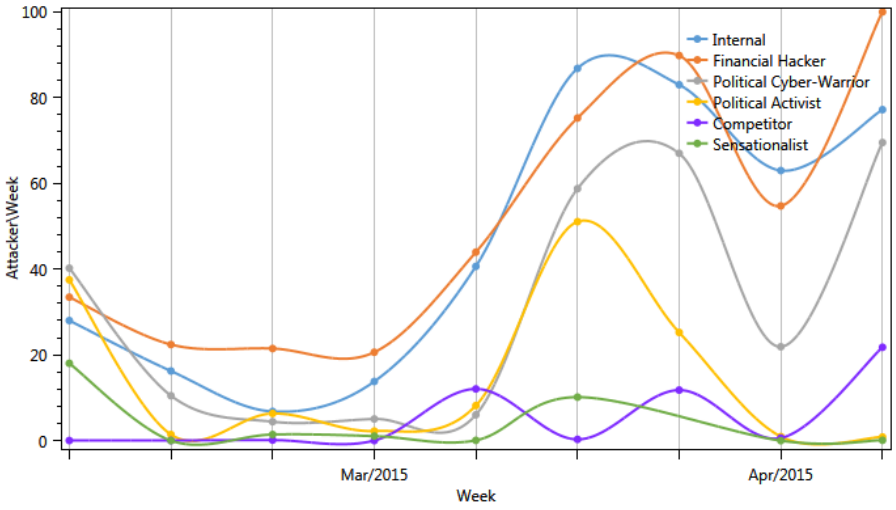
- DDoS refuses to die and is becoming a military-grade weapon, as seen in the Chinese “Great Cannon” which was apparently already used against Github.
- Interesting espionage campaigns were uncovered - one targeting the US Department of State and White-House, and the other coming from China and targeting government and media entities in south-east Asia.

Top trends

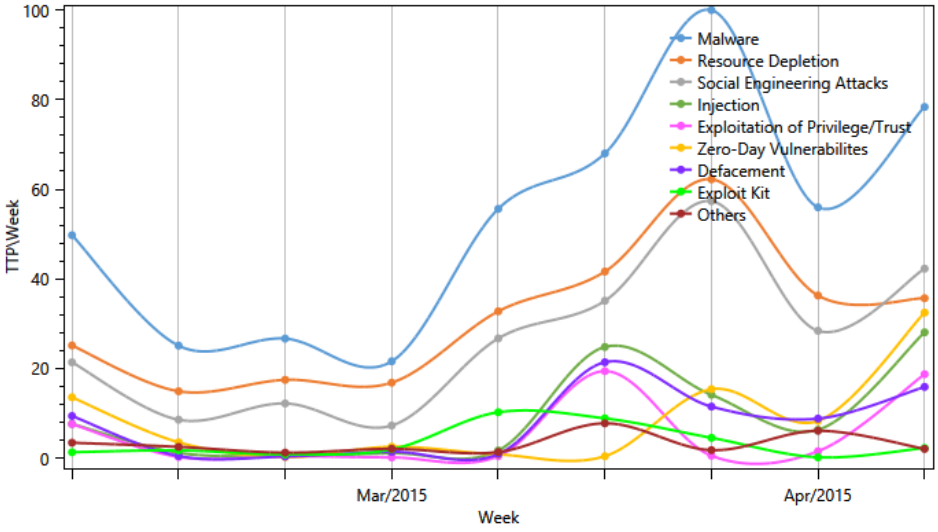
a. North-America Threat Landscape

When compared to March, April was significantly more active for most attackers in North-America, namely financial hackers, political cyber-warriors (nation-states and terrorists) and the insider threat.

While hacktivists and sensationalists were somewhat more active this month, mainly due to ricochets from OpIsrael and the conflict in Yemen, their activity level was low.



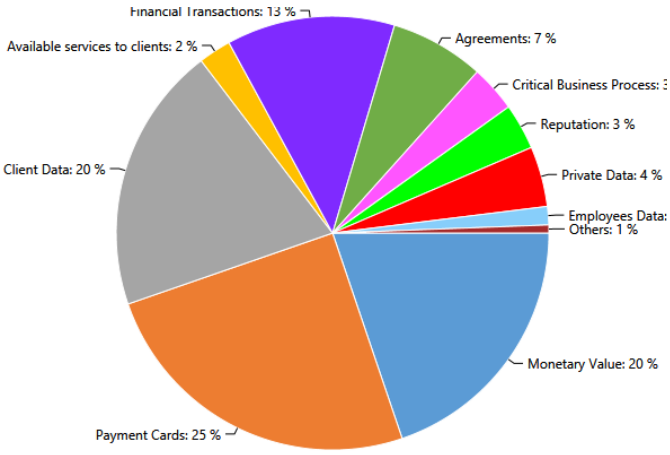
When looking from the prospective of TTPs it is clear to see a constant rising trend starting at the end of March and continuing all throughout April, as our system forecasted. The main TTPs which experienced the sharpest rise were malware, resource depletion and exploitation of privilege, with social engineering, zero-day vulnerabilities and injection as the main vectors.



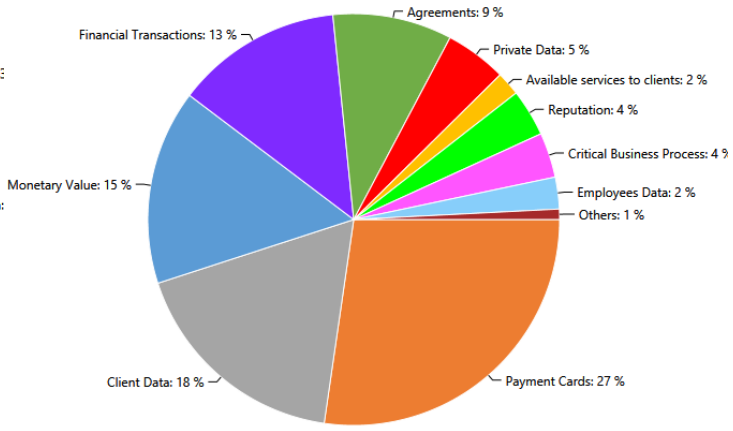
b. Most Targeted Assets

The most targeted assets on the attackers' scope this month were, as usual in recent months, Payment Cards, Personal Identifiable Information (Client Data) and "straight-forward" financial assets such as Monetary Value (bank accounts, Bitcoin, among others) and Financial Transactions. It is interesting to see that the Middle-East is becoming very similar to North America, when it comes to the targeted assets. This comes to show the shift that attackers have done to become geographically-agnostic and asset-focused.

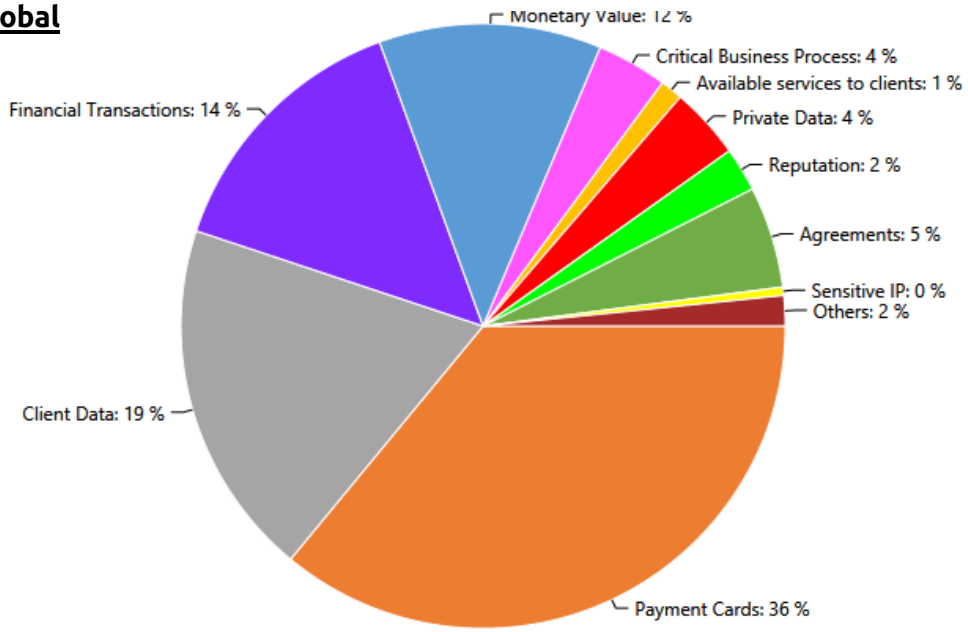
North America



Middle East



Global



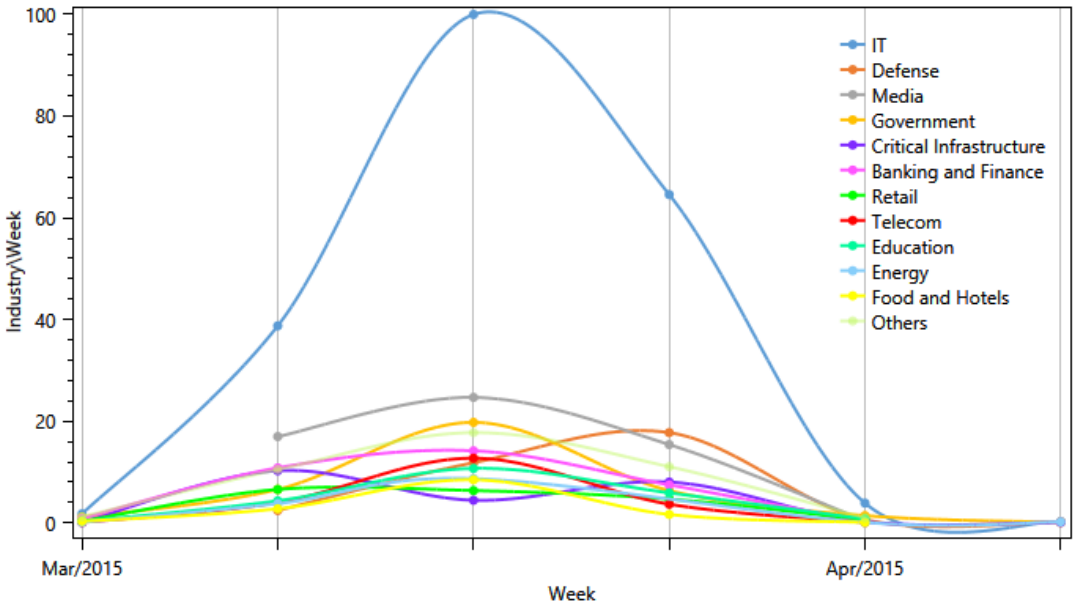
c. OpIsrael 2015

As in previous years, the Anonymous collective's Arab and Muslim affiliates, led by AnonGhost, conducted their annual OpIsrael campaign which peaked on April 7th. And again, as in previous years, the campaign ended with a whimper, without any major success or achievement. Actually, this year's campaign was even less successful than previous ones, perhaps due to better preparations on the Israeli side, and perhaps due to the abundance of ongoing campaigns conducted by the same attackers (against ISIS, against Al-Qaeda, surrounding the conflict in Yemen, to name a few).

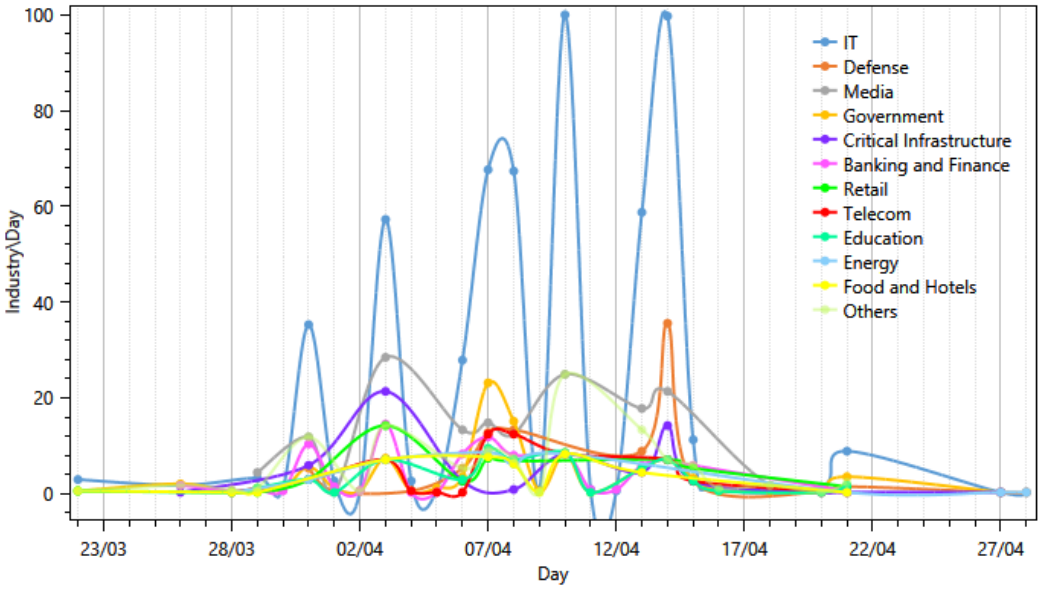
Nevertheless, there were some interesting things that popped out of the graphs:

- The attacks started to become severe a week before April 7th and in some cases lasted until, and even peaked, a week after.
- The IT sector (ISPs included) was predominant, followed by the likely suspects - media, banks and government. Looking at the daily view, the attacks on the IT sector had a strengthening wave pattern, with a couple of days between each wave.
- As usual, the top attack methods employed by the hacktivists were resource depletion, social engineering, defacements, injections and malware of different sorts.

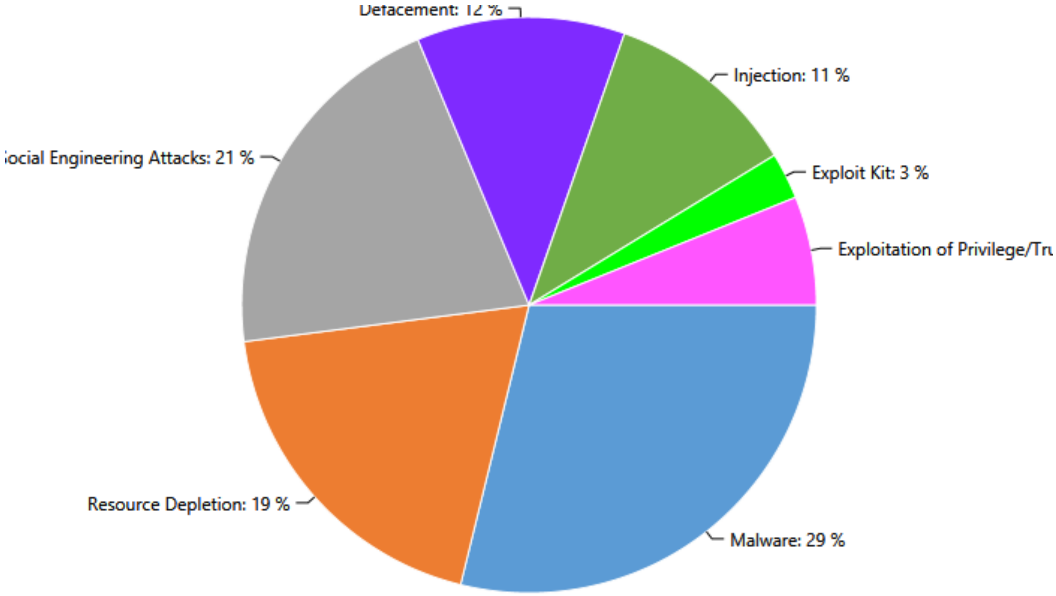
Threat Level by Industry (Weekly View)



Threat Level by Industry (Daily View)



Attack Methods Used



Main Incidents, Alerts and Developments

1. **DDoS as a Weapon** - Throughout 2014, different amplification techniques have been used by attackers in order to achieve larger and larger volumes per attack. A new research shows that attackers have been able to leverage SSDP (Simple Service Discovery Protocol) reflection amplification to achieve DDoS attacks larger than 100Gbps. The largest DDoS amplification attack since the beginning of 2015 was in India and it peaked at an astounding 325Gbps[1]. DDoS has become such a powerful and effective tool, that the Chinese government even developed what is dubbed "the Great Cannon" - a military-grade DDoS system which can produce crippling attacks. The tool has apparently been used by the Chinese government in order to block and censor anti-government websites - as was the case with the Github attack we mentioned in our previous intelligence update[2].
2. **Espionage**[3] **-** Two very interesting espionage campaigns have been uncovered this month:
    a. **The CozyDuke APT**[4] **-** Kaspersky published an APT group they dubbed as CozyDuke, which apparently was responsible for the breach into the US Department of State and White House's networks and email service. The group used spear-phishing attacks in order to redirect the targets to malicious websites and download a spyware. The group's techniques were similar to the known MiniDuke APT.
    b. **APT30**[5] **-** FireEye, for their part, uncovered a decade-long espionage campaign targeting south-east Asia. The campaign was conducted by Chinese attackers and targeted government, media, defense and other sectors in countries surrounding China. The attackers are highly capable; they implemented military-grade malware, backdoors, C&C and even targeted air-gapped systems, suggesting they are government-backed or affiliated.

[1] http://www.theregister.co.uk/2015/04/28/reflection_amps_drive_ddos_growth/
[2] http://www.hackersnewsbulletin.com/2015/04/great-canon-powerful-cyber-weapon-getting-used-china-government.html
[3] http://securityaffairs.co/wordpress/35181/cyber-crime/poseidon-pos-malware.html
[4] http://www.securityweek.com/cozyduke-apt-responsible-white-house-state-department-attacks-kaspersky
[5] http://www.securityweek.com/fireeye-uncovers-decade-long-cyber-espionage-campaign-targeting-south-east-asia