APT-C-36 recent activity analysis

lab52.io/blog/apt-c-36-recent-activity-analysis/

From Lab52 we have been tracking during the last months the activity of the group APT-C-36. This group was named and publicly introduced by the Company 360 [1] last year. In this article is highlighted as the main objective of the group, the companies located in Colombia. If you don't know APT-C-36, we recommend the article mentioned [1] for more information.

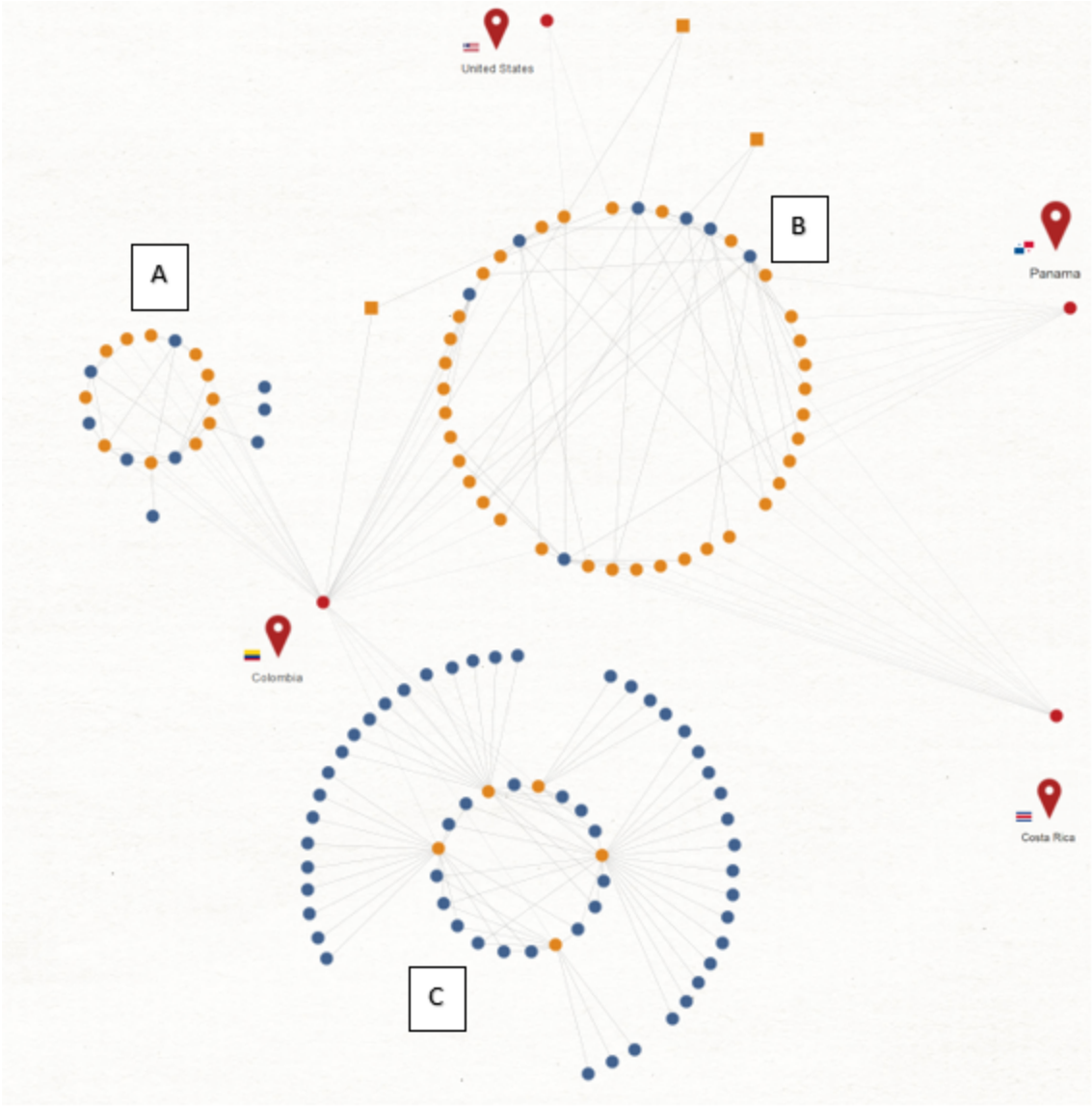
In July 2019 the company TrendMicro published an article related to another group [2] that also seems to be focused on Colombia and some **TTPs** (**T**actics, **T**echniques and **P**rocedures) overlap with APT-C-36 although TrendMicro indicates that they don't consider this group as an advanced.

Lab52 has had access to different very recent spear-phishings and the following summary information has been obtained from the analysis of these mails:

- This is a group that, as already mentioned in the articles [1] and [2], knows well the Spanish language.
- They usually use different types of url shorteners in their mailings. The case of "cort.as" shortenner has caught our attention since it is a shortener from the Spanish newspaper "El Pais" that belongs to the "Prisa Group" very spread in Latin America.
- We have also seen links to docs.google.com, mediafire and onedrive to download the samples inside some malspam emails.
- Their most popular malware is LimeRAT, although many others have been found as indicated in the reports. VJWorm has also been seen recently with different techniques for exfiltration.
- It has also been observed from some spear-phishings the exfiltration by Yopmail's HTTPS webmail service. This coincides with the indications of TrendMicro
- The most common dynamic domains seen are:
    1. duckdns.]org
    2. publicvm.]com
    3. linkpc.]net

Since Lab52 does not have enough information to be able to say that everything analyzed is a single group, it can only be said that these are different techniques used to attack a country.

From this information, the infrastructure used by the attackers as command and control servers when executing the malware has been analyzed and the following graph has been obtained:



Three sets (clusters) of ip addresses have been identified and each one has some characteristics:

Cluster A has the following characteristics:

- All its infrastructure is geolocated in Colombia. All the IPs correspond to Colombian ISPs' IPs. This is perhaps one of the most outstanding aspects.
- Domains are reused and the ip to which it points is changed.
- This cluster only uses free "duckdns.org" domains.

Cluster B has the following characteristics:

- Its infrastructure is located in Colombia, Costa Rica and Panama. The geolocated ip's in the United States correspond to domains that have been "sinkholed". By obtaining more information about the IPs, it can be seen how they are using a VPN service that allows having geolocalized IPs in Colombia, Costa Rica and Panama. The service is called "Powerhouse Management" (phmgmt[.]com). Therefore this cluster is not compromising infrastructure of Colombian ISP clients, but is using this VPN service.
- This cluster is reusing domains and changing ip addresses a lot. They have a very short duration.
- This cluster uses as SLD linkpc.net and publicvm.com.
- This cluster coincides with part of the domains registered in the report of the Chinese company 360 on APT-C-36.

Cluster C has the following characteristics:

- All its infrastructure is geolocated in Colombia. All the IPs correspond to Colombian ISPs' IPs.
- In this case many domains are used and few ip addresses.
- This cluster uses free domains duckdns.org.

Among the domains used by these group/s we highlight the domain:

> **cobroserfinansa[.]com**: This domain has solved more than 150 different ip's (157 exactly when this report was made) where all of them have been located in Colombia.

Another outstanding aspect from the infrastructure point of view is that the ip's located in Colombia correspond with a high probability to ip's of routers compromised by the attackers. Lab52 hypothesis is that attackers compromise routers with default credentials and use them as a frontend for their real command and control server. This fact has not been verified by Lab52, but has been observed as a common TTP for other groups. The routers seen, allow the use of the iptables command so automation by attackers for redirection is simple.

Conclusions

- The attackers know well the language of the attacked country, Spanish, so it could be considered Spanish-speaking countries as the main options of attacking countries. This aspect has already been indicated in the other reports. From Lab52 we would reinforce this hypothesis by the use of a shortener "cort.as".
- The emails are well written and are almost always related to financial matters, specifically related to debt.
- Currently, the attackers are not using malware developed by themselves and are using public malware projects such as LimeRAT.
- Attackers are using high ports to communicate with command and control servers.

- Attackers are probably using multi-level command and control architectures to hide the main command and control server. As a first level, they have used until the moment:
    - VPN services where Colombia, Panama and Costa Rica exist as an outgoing ip
    - Routers from ISP clients with default credentials or vulnerabilities. All these ISPs belong to Colombia.
- Attackers use shorteners for links in emails. It is advisable to watch out for shortcuts belonging to the newspaper “El Pais”.
- Another option to the shorteners are links to file hosting services (google, mediafire, dropbox, etc.)

[1] https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

[2] http://blog.la.trendmicro.com/proyecto-rat-una-campana-de-spam-dirigida-a-entidades-colombianas-a-traves-del-servicio-de-correo-electronico-yopmail/