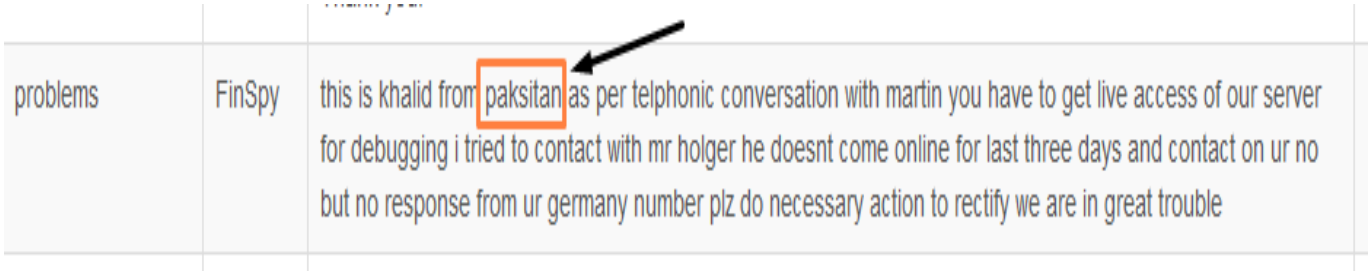
An Analysis of “Spyfiles 4” – An Indian Perspective

Recently Wiki leaks released a set of documents and files regarding the “FinFisher” spying system. FinFisher is a product line (developed by a private company) that is used by Governments worldwide to spy on Journalists, Activist, Opposition Parties etc.

In this report we are going to list a few details that might be shed an “Indian Perspective” to all this information.

Customer Username: 0DF6972B

All these products were sold to a person/organization in Pakistan. It should be noted that Finspy does not sell to any non-governmental organization.



problems	FinSpy	this is khalid from paksitan as per telphonic conversation with martin you have to get live access of our server for debugging i tried to contact with mr holger he doesnt come online for last three days and contact on ur no but no response from ur germany number plz do necessary action to rectify we are in great trouble

Licenses

Software	Start	Expiration	Estimated Cost
FinSpy	2010-04-20 00:00:00	2013-04-30 00:00:00	Base license + 35 targets + 5 agents €396900
FinFly USB	2010-04-20 00:00:00	2013-04-30 00:00:00	€4620
FinIntrusion Kit	2010-06-08 02:00:00	2013-06-10 02:00:00	€30600

The FinSpy product is capable of bypassing all major anti-viruses and has the following “features”

- Works on Linux , Macintosh and Windows
- Intercept Skype
- Log keystrokes (Keylogging)
- Monitor Screen
- Seal Files from the computer
- Monitor webcam and microphone
- Trace Location
- Makes use of proxies to avoid detection

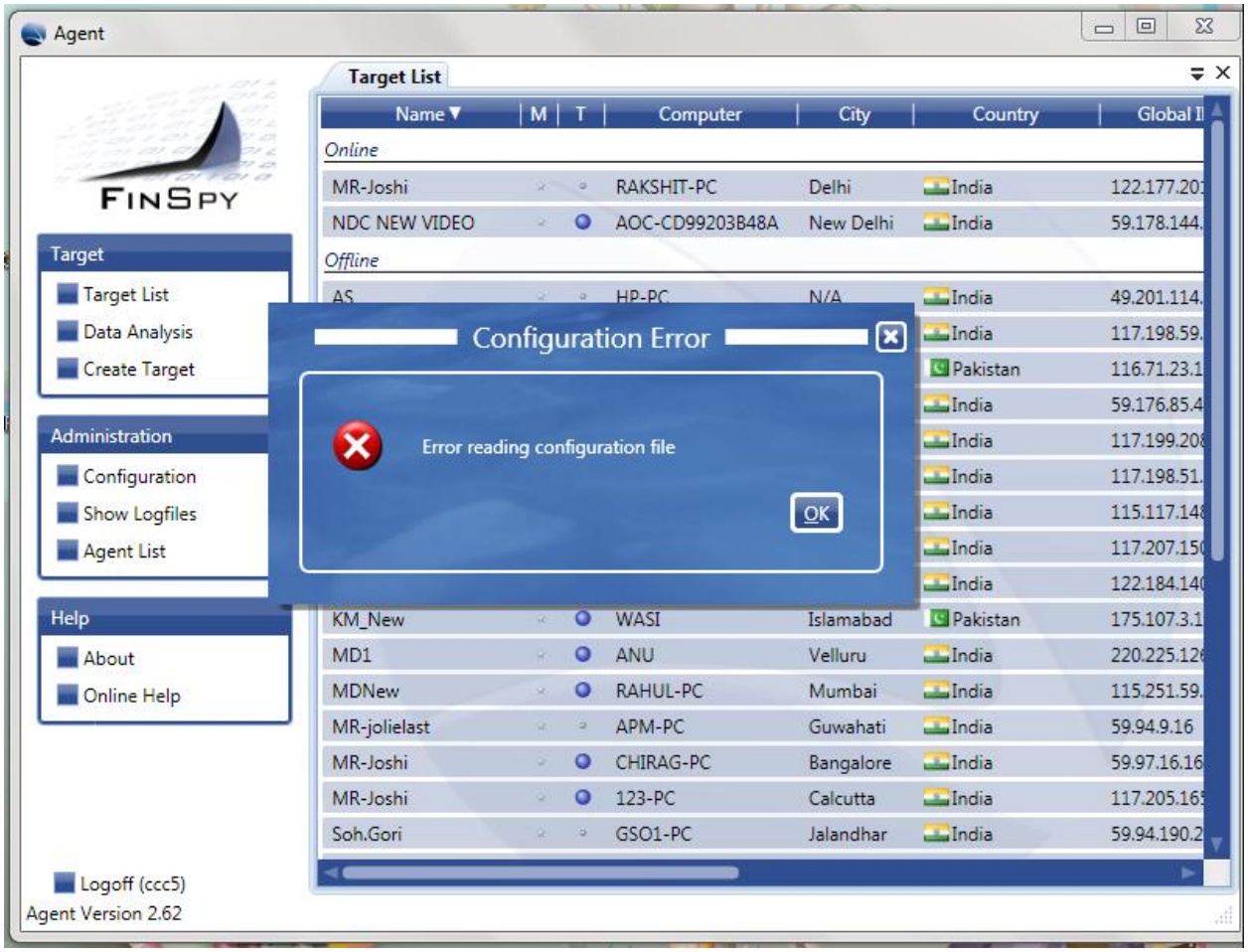
The Fin USB product that is used to deploy the “FinSpy” software on a victim’s computer when there is physical access. (Seems to point that they had physical access to Indian Computers)

- Deploys “FinSpy” software on the victim
- Bypass Truecrypt
- Works even is computer is turned off
- Looks and acts like a normal USB stick

The FinIntrusion Kit has the following features

- Crack WirelessNetwork (WEP, WPA 1, WPA 2)
- Intercept the following information via WLAN (Passwords, Usernames, Uploded/Downloded files, URL’s visited etc)
- Jamming of legitimate Wifi access points.
- Fake Access Points
  (The Fin Intrusion attacks can only be done if the target is in the general vicinity of the attacker)

If you look at the screenshot (https://wikileaks.org/spyfiles4/attachments/B1EA1F1E.png) you can see there are 16 Indian IP's and only 2 Pakistani IP's .So there is limited "domestic" use.



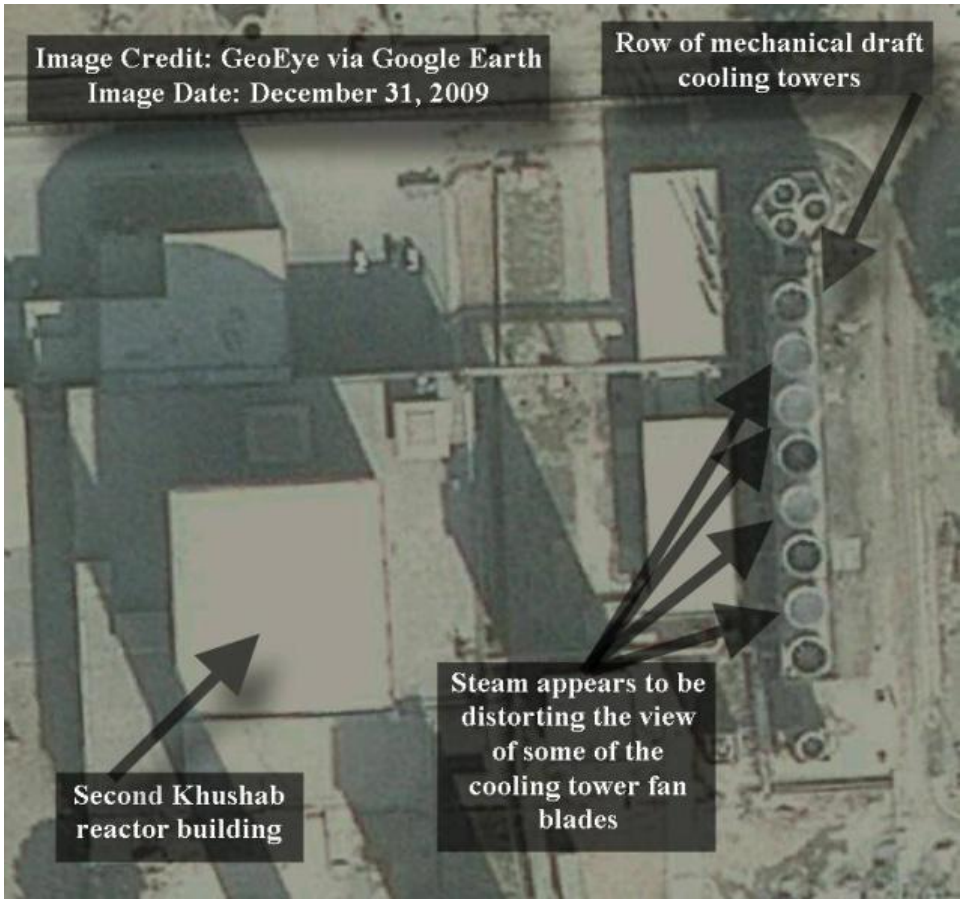
The partial IP addresses of all the victims are shown in the screenshot.

Also the window has more victims when scrolling down. By taking into account the "unscrolled" area we are able to calculate that there are 10 more victims so thus bring the total number of victims to ≈ 28. From the IP an organization like CERTIn should be able to identify the approximate PC which has been infected. Finfisher may have advanced polymorphic cryptors which may make detection difficult with antivirus software. We recommend working on special identification software and sweep on all government of India computers.

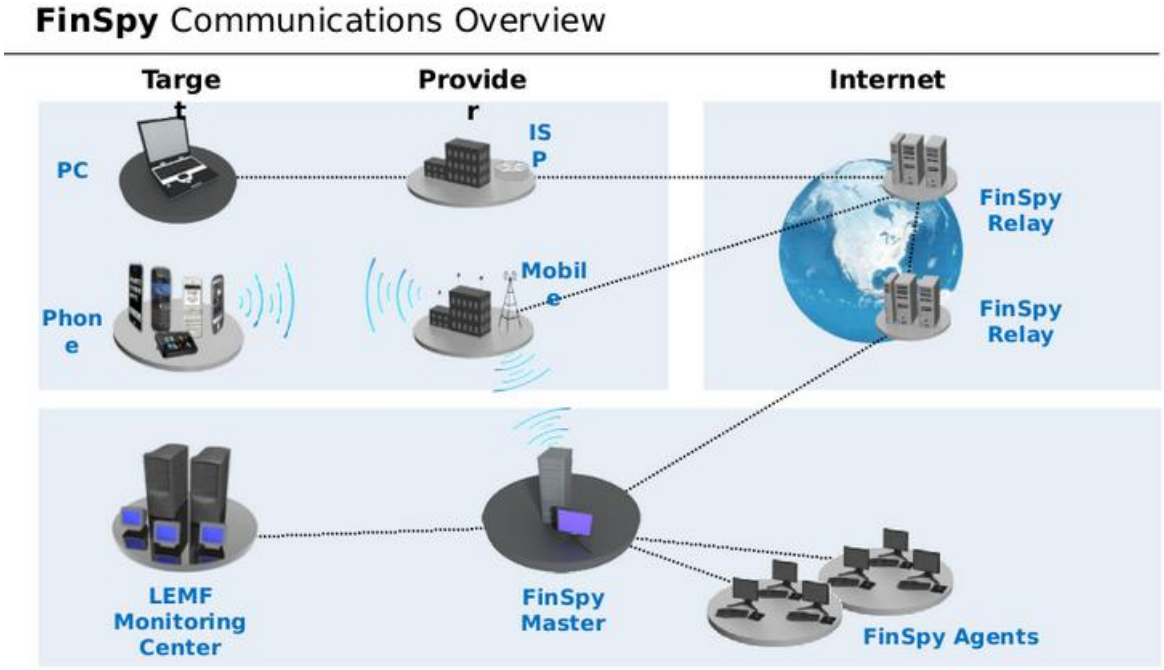
The questions posed by the customer seem to indicate that they were actively doing the attack and were exfiltrating important data from the victims, that too in large amounts.

Offline download managment and Incremental downloads	FinSpy	We are happy that the feature of offline target configuration has been added already. It is working successfully at our side. Earlier we have requested another feature which is described below. We would be pleased if Gamma can add a feature in which the agent be able to select files to download even when the target is offline and whenever the target comes online, those selected files may be downloaded without the interaction required from user. Also presently, the downloading of files discontinues if there is a network disconnect error or any other error. That file has to be downloaded again from scratch. This is a real annoyance. We want that when the connection is lost between target and agent, the file download pauses automatically wherever it was and whenever the target comes online again, the download starts from the point where it paused. In this way a lot of effort and time can be saved. It is also useful for the files which are slightly bigger than usual. I call this feature incremental download. I hope Im correct in that. Thank you

One of the Exe's leaked by Wikileaks "finfisher.2.zip" MD5: 074919f13d07cd6ce92bb0738971afc7 when opened shows the image of "khushab nuclear reactor" in Pakistan. This might have been used to target Indian Officers as they might be tempted to click on it and view the image.



In the event that it is detected and analyzed, FinFisher makes use of Proxy and Relaying techniques in order to hide the location the master controller (attacker).



Analysis:
https://anubis.iseclab.org/?action=result&task_id=1dec5f771b00eca749d0a22c7df9fa6e9&format=html

https://drive.google.com/file/d/10NPnbpaAbq1U_i-nsYo6ceGF2U0UKYrTz9tqVVM7My_MDEo-OnydyqM_AmOB/edit?usp=sharing

Conclusion:

We recommend Government of India to take immediate steps to develop specialized scanners which can identify/protect against finfisher attacks from neighboring countries. Most antivirus companies only use MD5 hashes to identify the spyware on computers. This is not enough as Finfisher is able to create another version (of the software with a new Md5 hash), so identification/protecting becomes difficult.