DarkComet Tracker

Degree programme: BSc in Computer Science | Orientation: IT-Security
Thesis advisors: Dr. Endre Bangerter, Reto Inversini
Expert: Dr. Igor Metz (Glue Software Engineering AG)

RATs are the so called Remote Access Trojans. They allow the people behind them, also termed operators, to remotely access to a victim's computer that has previously been infected. This can then be spied on, manipulated or totally taken over. Several RATs are available for free or at low prices on the Internet. Their user-category ranges from script-kiddies to intelligences, in a context like the war in Syria. The main topic of our work is the RAT DarkComet.

Main Goals

Get RAT-samples from the wild, find active operators and infect our real-looking victims in order to determinate their behaviour.

Infection Process

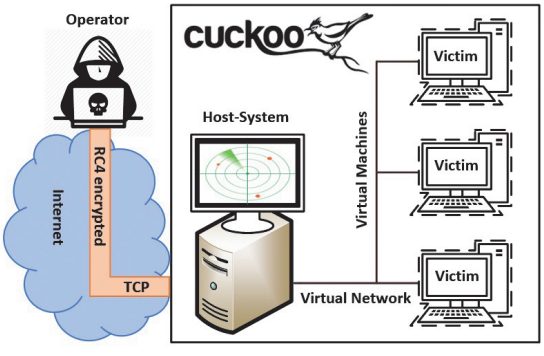
The most difficult phase for Operators, in order to achieve their goals, is the infection process. In fact, the RAT sample needs to be delivered to the victim, in order to be manually executed (double click). Once executed, the RAT sample tries to create a connection to the Operator's host and port, using its own configuration. Moreover, the network connection is usually encrypted, using SSL/TLS or other protocols. In our case, DarkComet encrypts the network connection, using the RC4 algorithm and a pre-shared key.

Implementation with Cuckoo

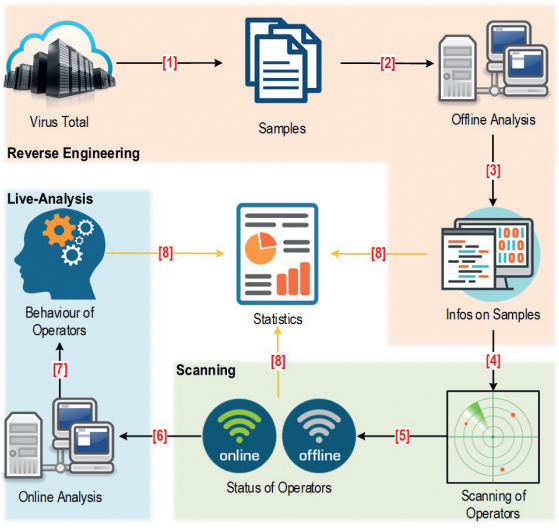
Cuckoo Sandbox is «the leading open-source automated malware analysis system». In fact, it uses a series of utilities, such as virtual machines, virtual memory tools, network traffic analysers and others to analyse and report malware samples.
We regularly download samples from VirusTotal (1) and analyse them to check whether they are DarkComet samples or not (2). In the positive case we extract and store the configuration of the sample (3), containing all the important information. The extracted addresses of the hosts are then regularly scanned (4), to determinate whether the operator is online or offline (5). For online operators, we submit their RAT sample to the Cuckoo Sandbox and analyse it in live-mode. After a self-infection, we let the operators connect and take control of our virtual machines (6). We record the analysis and create dumps of the network traffic. In a second time, we decrypt the network traffic, using the password previously extracted from the sample configuration. We analyse which commands have been executed by the operators (7). Based on this data, we categorize operator's behaviour (8).

Results

- Download of 2441 malware samples from Virus Total, 746 DarkComet configurations extracted
- 101 895 550 unique IP scanned worldwide and 1312 operators tracked
- Operators from 80 countries
- 741 live analyses, 932 minutes of operator's interaction



Simple Project Infrastructure



DarkComet Tracker Data Flow

Nils Stampfli
nils.stampfli94@gmail.com

Sandro Tiago Carlao
tiago.sandro@hotmail.com

Rosalie Truong
rosa.g@windowslive.com