Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal IT Steering Unit FITSU
Service for Analysis and Prevention SAP

Reporting and Analysis Centre for Information Assurance MELANI

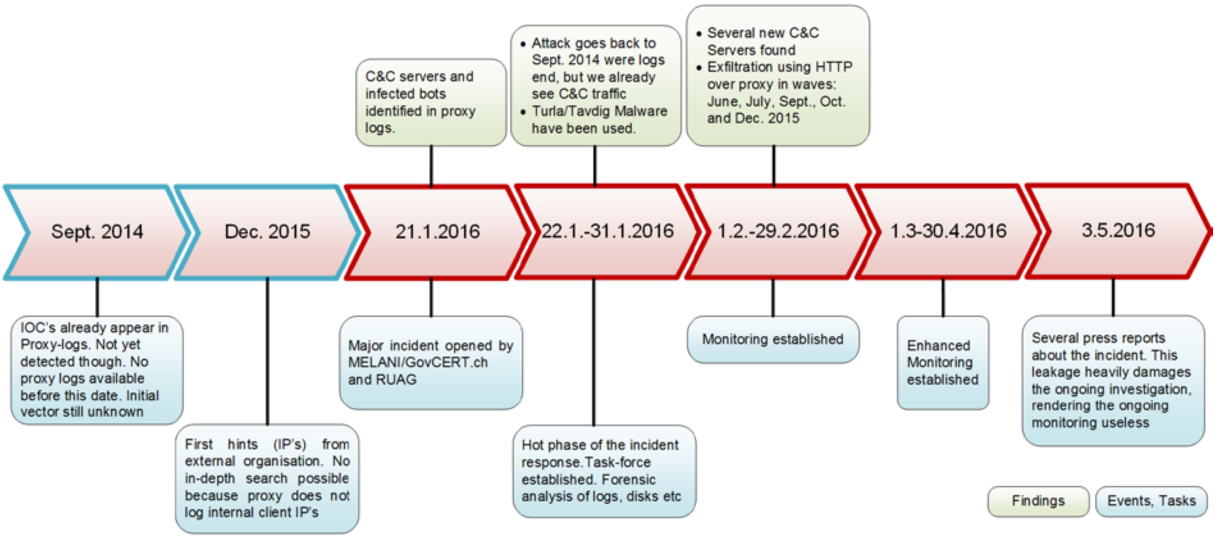
Summary: Technical Report about the Espionage Case at RUAG

The RUAG cyber espionage case has been analyzed by MELANI/GovCERT in order to provide insight and protection. The Federal Council has decided to publish this report to give organizations the chance to check their networks for similar infections, and to show the modus operandi of the attacker group.

The attackers have been using malware from the Turla family, which has been in the wild for several years. The variant observed in the network of RUAG has no rootkit functionality, but relies on obfuscation for staying undetected. The attackers showed great patience during the infiltration and lateral movement. They only attacked victims they were interested in by implementing various measures, such as a target IP list and extensive fingerprinting before and after the initial infection. After they got into the network, they moved laterally by infecting other devices and by gaining higher privileges. One of their main targets was the active directory, as this gave them the opportunity to control other devices, and to access the interesting data by using the appropriate permissions and group memberships. The malware sent HTTP requests to transfer the data to the outside, where several layers of Command-and-Control (C&C) servers were located. These C&C servers provided new tasks to the infected devices. Such tasks may consist of new binaries, configuration files, or batch jobs. Inside the infiltrated network, the attackers used named pipes for the internal communication between infected devices, which is difficult to detect. This way, they constructed a hierarchical peer-to-peer network: some of these devices took the role of a communication drone, while others acted as worker drones. The latter ones never actually contacted any C&C servers, but instead received their tasks via named pipes from a communication drone, and also returned stolen data this way. Only communication drones ever contacted C&C servers directly.

It is difficult to estimate the damage caused by the attackers; this is by any means beyond the scope of this report. However, we observed interesting patterns in the proxy logs. There were phases with very few activity, both in terms of requests and amount of data transferred. These quiet phases were separated by high-activity periods with many requests and big amounts of exfiltrated data.

In the report, we provide some recommendations and countermeasures we consider most effective against this kind of threat on the level of end-devices, the active directory, and the network. It is important to mention that many countermeasures are not cost-intensive, and can be implemented with reasonable amount of work. Even if it is difficult to completely protect an organization against such actors, we are confident that they are detectable, as everyone makes mistakes. The defending organization must be ready to see such traces, and to share this information with other parties, in order to follow such attackers closely.



Sept. 2014

IOC's already appear in Proxy-logs. Not yet detected though. No proxy logs available before this date. Initial vector still unknown

Dec. 2015

First hints (IP's) from external organisation. No in-depth search possible because proxy does not log internal client IP's

21.1.2016

C&C servers and infected bots identified in proxy logs.

Major incident opened by MELANI/GovCERT.ch and RUAG

22.1.-31.1.2016

- Attack goes back to Sept. 2014 were logs end, but we already see C&C traffic
- Turla/Tavdig Malware have been used.

Hot phase of the incident response. Task-force established. Forensic analysis of logs, disks etc

1.2.-29.2.2016

- Several new C&C Servers found
- Exfiltration using HTTP over proxy in waves: June, July, Sept., Oct. and Dec. 2015

Monitoring established

1.3-30.4.2016

Enhanced Monitoring established

3.5.2016

Several press reports about the incident. This leakage heavily damages the ongoing investigation, rendering the ongoing monitoring useless

Findings

Events, Tasks