Contribution ID: **64** Type: **Oral Presentation**

Divide and Conquer: Distributing delivery of large Security Challenge payloads

Tuesday, 2 April 2019 17:00 (30 minutes)

In Security Service Challenges the readiness of an infrastructure's incident response capability is assessed. Here we simulate a situation where a legitimate credential is used for activities violating various policies, requiring the involved security teams to take action in order to resolve the incident. An important part here is the containment of the malware, which would be easily doable if the attacker would use the standard grid job submission systems. Therefore, an external delivery system is needed.

For the EGI Security Service Challenge, we explored using BitTorrent as a way to reliably deliver the software needed to connect to the Tor network. A number of initial 'seedboxes' were set up in different countries, which announced their availability to a private 'tracker'.

This tracker, hidden as a Tor service, could be reached through either a public Tor proxy, or through the Tor network. As a fallback to the peer to peer delivery system, the torrent file also contained a number of 'web seeds', http(s) mirrors that are being served for the Tor Project.

As the BitTorrent client checks for data integrity, there is some level of guarantee that the software has been delivered correctly and the web seeds are valid. We used the aria2 download utility on the to-be infected machines as it is light weight, well maintained, hosted on the generally available GitHub, and written in such a way that it relies solely on generally available libraries and technologies. Aria2 was built on the machines themselves to account for subtle differences among the grid infrastructures across the sites.
In an attempt to hide most of the infected nodes, not all the systems will start seeding after they have finished downloading. This makes the forensics more of a challenge the infected nodes cannot just be requested from the tracker.

Primary authors: ROORDA, Jouke (Nikhef); Dr GABRIEL, Sven (Nikhef/EGI)

Presenter: ROORDA, Jouke (Nikhef)

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations