Projektsitzung 23. September 2016

Datum	23.09.2016
Zeit	8:00–9:00 Uhr
Ort	Compass Security, Werkstrasse 20, 8645 Jona SG
Anwesende	Ivan Bütler
	Fabian Binna
	Silvan Adrian

Traktanden

- Abgrenzung der Arbeit: Nur Erkennung C&C?
- Lösungsansätze: Data Mining? Machine Learning?
  Nur Analyse des Netzwerkverkehrs erlaubt bzw. nur Proxy
- Ziel der Arbeit? Umfang der Abgabe? Proxy Software, Analyse?
- Testumgebung? Vorhanden, selber aufsetzen?
- Testen der Lösung? Diverse Trojaner? Diverse Testumgebungen? Netzwerkaufzeichnungen zum testen?
- Zugriff auf Repository, Jira ...
- Termine für weitere Besprechungen (Sprints)? Intervall?
- Private Repositories?
- Bewertungsbogen?
- Nächste Schritte

Was wurde erreicht

- Aufsetzen der Dokumentation
- Einarbeiten ins Thema APT
- Aufsetzen der CI Umgebung

Beschlüsse

- keine public Repositories (Minimum: Lösung des Problems, Programcode des Fake C&C)
- Nächster Termin 30.09.16 9:00 - 10:00 Uhr

Weiteres Vorgehen

- Sprint 1 planen
- Eigener Client-Server mit Fake C&C (Zu Demonstrationszwecken)
- Umbau Infrastruktur (Private Repositories)