Projektsitzung 30. September 2016

Datum	30.09.2016
Zeit	9:00–10:00 Uhr
Ort	Compass Security, Werkstrasse 20, 8645 Jona SG
Anwesende	Ivan Bütler
	Fabian Binna
	Silvan Adrian

Traktanden

- Fake C&C Varianten
- IP Adressen und oder Domain Namen der C&C Server bekannt?
- C&C Server blocken vs. Paket vom Trojaner abfangen

Was wurde erreicht

- Anforderungen für Prototyp festgelegt
- Angefangen mit der Proxyanalyse
- Kleiner Prototyp programmiert

Beschlüsse

- Variante 2 nicht möglich (Mix aus beiden Varianten)
- Sitzungen mit Präsentation beginnen (roter Faden für die Sitzungen)
- Aufgabenstellung wird zugestellt

Weiteres Vorgehen

- Sprint 1 fortsetzen
- Variante 1 und 2 zu einer Variante umbauen
- Bessere Lösung finden als mitmproxy
- Analyse um Requests direkt an Fake C&C weiter zu senden (reset 3 Way Handshake)