HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

HS2016

BA

September 30., 2016

Document Name:	Aufgabenstellung_BA_Fake_C_AND_C.docx
Version:	v1.0
Author	Ivan Buetler
Date of Delivery:	September 30., 2016
Classification:	BA

Table of Content

HSR Hochschule für Technik
Postfach 1475
CH-8640 Rapperswil
www.hsr.ch

1 Ausgangslage

1.1 APT Angriffe

Im Kontext von APT versuchen Cyber Kriminelle und Intelligence Services geheime Informationen aus dem Firmennetz ins Internet zu exfiltrieren. Dies wird oft auch als Command und Control (C&C) Verbindung bezeichnet und bei professionellen Angreifern mehrschichtig eingesetzt. Das zwingt die Unternehmen, sich mit dem Verhalten des Netzwerkverkehrs von innen nach aussen auseinander zu setzen und sich zu überlegen, wie man bösartigen Traffic erkennt und damit umgeht.

Ein möglicher Ansatz für die Erkennung von C&C Verkehr besteht in der intelligenten Korrelation von Log Daten. Mit Software wie Splunk oder Elasticsearch stehen Tools zur Verfügung, die sich hierfür anbieten. Grundsätzlich geht es darum die echten Log Daten des Unternehmen (DNS, Proxy, Firewall, DHCP) mit Indikatoren aus dem Internet (IP Reputation, Virustotal, Malware.lu, Realtime Blacklist) abzugleichen und die Fähigkeit zu erwerben, mit geeigneten Splunk Abfragen die Malware zu erkennen.

Das ist aber noch nicht genug. Wie geht man damit um, wenn eine Malware erkannt wird? Wie kann man die infizierten Maschinen im Glauben lassen, dass der Angriff noch nicht erkannt wurde? Wie sieht eine Lösung aus, welche die Umleitung von C&C Traffic auf einen Fake Server ermöglicht?

1.2 Auftrag

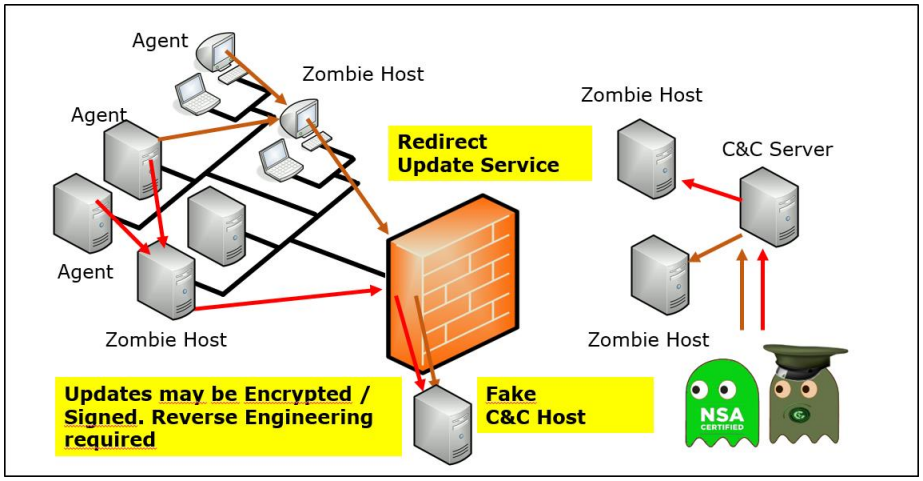
Im Rahmen von dieser HSR Bachelor Arbeit soll eine Methodik mit Tool entwickelt werden, um bei Befall von APT besser reagieren zu können. Das Tool soll den C&C Traffic analysieren und an einen Fake C&C weiterleiten können. Einige weiterführenden Details und Anforderungen findet man im nächsten Kapitel.

1.3 Voraussetzung

Das System soll in einem Umfeld eingesetzt werden, welche einen sogenannten SSL Splitting Proxy betreibt. Das sind spezielle Content Filter Proxies (Bluecoat, WebWasher, u.ä) welche den SSL Verkehr zwischen Client und einer SSL/TLS Anwendung analysieren um den Inhalt auf Virus und Trojaner zu untersuchen. Das System funktioniert analog einem Inspection Proxy wie ZAP, Burp oder auch dem Linux mitm Tool.

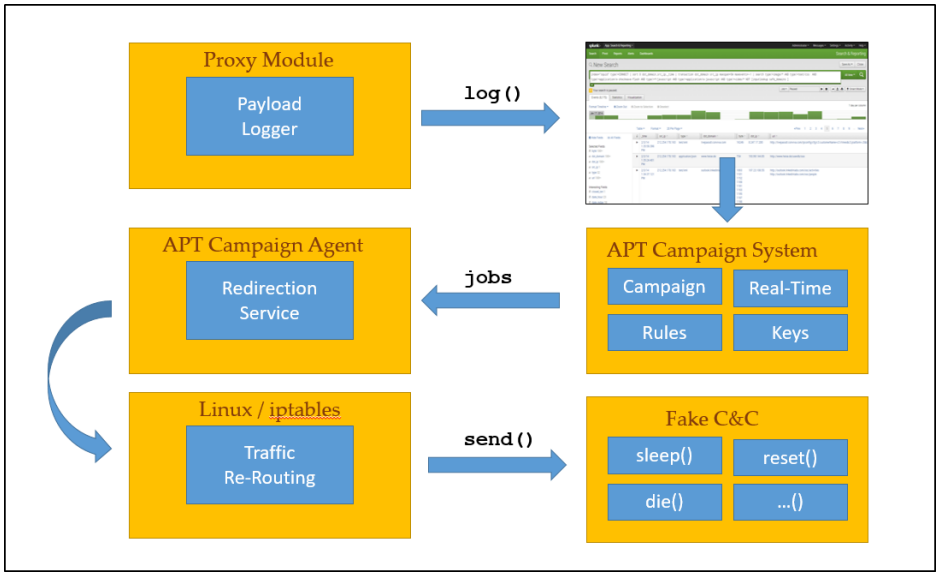
HSR Hochschule für Technik
Postfach 1475
CH-8640 Rapperswil
www.hsr.ch

1.4 Beispiel



Im Beispiel oben versuchen die infiszierten Clients via Firewall (SSL Splitting Proxy) auf den C&C im Internet zuzugreifen. Da die C&C Verbindung eine gewisse Charakteristik aufweist, sollen die Verbindungen zum C&C zum Fake C&C rerouted werden. Alle anderen Verbindungen vom Client in das Internet sollen nicht über den Fake C&C laufen.

1.5 Möglicher System Ansatz



Der Payload Logger schickt die Payloads der Verbindungen zu einem Splunk ähnlichen System. Das APT Campaign System analysiert diese in Real-time und versucht den C&C Traffic zu entschlüsseln. Hierzu kann der Kampagne Schlüssel und Algorithmen hinzugefügt werden. Aus der Analyse der Payloads generieren sich Jobs, welche beim APT Campaign Agent zu einer Redirection führen.

HSR Hochschule für Technik
Postfach 1475
CH-8640 Rapperswil
www.hsr.ch

1.6 Mögliche Herausforderungen

Die Verbindungen zwischen infisziertem Client und dem C&C können verschlüsselt sein. Möglicherweise ist der Payload auch mehrfach und mit unterschiedlichen Algorithmen verschlüsselt. Um eine Redirection zu initiieren, sind die TCP/IP 3-Way Handshakes als auch die SSL Verbindungen zu berücksichtigen, die allenfalls schon aufgebaut oder neu initiiert werden müssen. Der Fake C&C muss die Logik des C&C kennen, um diesen imittieren zu können.

1.7 Erwartetes Ergebnis

Die Bachelor-Arbeit soll im theoretischen Teil analytisch beleuchten und analysieren, wie die Lösung einer Fake C&C Umgebung umgesetzt werden könnte, unter Berücksichtigung der obig dargestellten Ausgangslage. Hierbei wird eine wissenschaftliche Vorgehensweise und Dokumentation erwartet.

Im praktischen Teil soll eine funktionierende PoC Lösung entwickelt, getestet und bewertet werden. Diese soll im Kontext einer bereits vorliegenden Malware mit C&C einsatzbereit sein. Die Malware selbst mit C&C ist demnach nicht Bestandteil der Aufgabe. Die Test-Malware kann über einen HTTP-Proxy arbeiten und hat für sich selbst auch Payload Encryption aktiviert. Die Malware ist für Microsoft Windows ausgelegt.

Die Testing Ergebnisse müssen für den Leser der Bachelor Arbeit nachvollziehbar sein. Das heisst, der Setup der Tests, die Details des Tests, die Darstellung von erwarteten und getesteten Testpunkten müssen ersichtlich und nachvollziehbar sein. Idealerweise sind die Tests mit den Use-Cases der Lösung verlinkt.

Darüber hinaus gelten die von der HSR publizierten Anforderungen an die Dokumentation einer BA-Arbeit.

1.8 Vertraulichkeit

Sämtliche Informationen über die Malware sind als vertraulich gekennzeichnet und dürfen zu keiner Zeit öffentlich oder Dritten zugänglich gemacht werden. Die Ergebnisse der BA-Arbeit mit dem theoretischen und praktischen Teil sind nicht vertraulich. Sämtliche Dokumentation im Zusammenhang mit der Malware (Testing, Fake C&C) sind als vertraulich zu erachten und dürfen nicht öffentlich gemacht werden.

HSR Hochschule für Technik
Postfach 1475
CH-8640 Rapperswil
www.hsr.ch