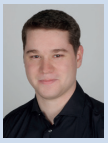
Silvan
Adrian

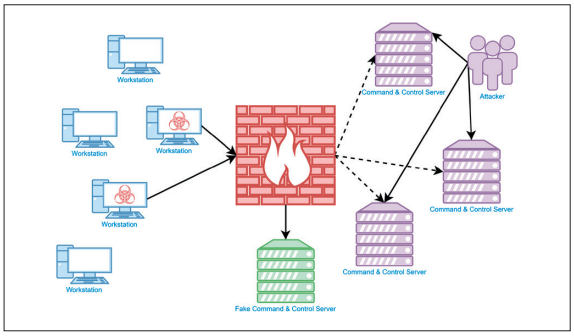


Fabian
Binna

Diplomanden	Silvan Adrian, Fabian Binna
Examinator	Ivan Bütler
Experte	Daniel Frei, SwissRe
Themengebiet	Internet-Technologien und -Anwendungen

Proxy Redirection with Fake C&C

Schadensverminderung und Zeitgewinnung bei APT-Attacken



Implementierter Lösungsansatz – Umleitung der Malware-Kommunikation auf einen Fake-Command&Control-Server

Verwendete Technologien

Softwarelösung zur Aufgabenstellung

Ausgangslage: Unter dem Begriff Advanced Persistent Threat (APT) versteht man gezielte und langfristig geplante Cyber-Attacken, so wie es das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) und die RUAG im Jahre 2016 erlebten. Wenn eine APT-Attacke identifiziert wird, dann stehen zeitraubende Analysearbeiten an, während denen der Angriff weiter fortschreitet. Es stellt sich die Frage, wie der Angriff verhindert oder zumindest verzögert werden kann, ohne dass die Täterschaft dieses Eingreifen bemerkt.

Vorgehen/Technologien: Diese Bachelor Arbeit stellt eine Methodik und ein Tool vor, wie der Schaden im Unternehmen reduziert, und gleichzeitig die Chancen für ein Unerkannt bleiben bei der Täterschaft erhöht werden können. Im Wesentlichen handelt es sich um ein Verfahren, um Zeit zu gewinnen, damit die APT-Attacke im Detail untersucht werden kann, ohne weiteren Schaden zu riskieren.

Ergebnis: Das Resultat der Arbeit umfasst eine Software, die es erlaubt, durch Trojaner (Malware) infizierte Clients im Unternehmensnetzwerk zu erkennen und stillzulegen. Die Malware ist aus Sicht des Angreifers funktionsfähig, in der Tat ist die Malware jedoch im Sleep-Mode, ohne dass dies vom Angreifer bemerkt wird. Somit gewinnt das betroffene Unternehmen Zeit, um den Fall im Detail zu klären und die Gefahr, die durch die Malware für das Unternehmen entsteht, abzuwenden.