Details zur APT-Gruppierung „Inception Framework“

	Risiko ■■□□□
Sachstand:	Symantec hat die Angriffsmethoden der Gruppe „Inception Framework” analysiert. Inception Framework ist eine Gruppierung, die seit etwa 2014 aktiv ist und bereits mehrere erfolgreiche Spionage-Kampagnen durchgeführt hat. Eine der wesentlichen Fähigkeiten von Inception Framework ist die Verschleierung ihrer Identität. Durch kompromittierte Router werden kurzlebige Router-Kaskaden („Router“-Proxies) aufgebaut und ausspionierte Daten über verschiedene Wege transportiert. Der Infektionsweg geschieht per E-Mail über manipulierte Office-Anhänge, die Schwachstellen in der Microsoft Office Suite ausnutzen, zum Beispiel: • CVE-2014-1761: Remote Code Execution durch manipulierte RTF-Dateien (CVSSv2: 9.3) • CVE-2012-0158: Remote Code Execution durch manipulierte RTF-Dateien, Webseiten oder Office-Dokument (CVSSv2: 9.3) Inception Framework nutzt legitime Cloud-Anbieter, um die abgegriffenen Daten zu empfangen. Begonnen wurde mit einem Cloud-Anbieter, die Anzahl ist in den letzten Jahren stetig gewachsen.
Bewertung:	Die Bedrohungslage durch APTs wurde im Rahmen des CSCC bereits mehrere Male bewertet. APTs stellen kontinuierlich eine hohe Bedrohungslage für Unternehmen dar. Abhängig vom Ziel und Zweck der APT (Spionage, Wiper etc.), der Branche des Unternehmens und der geographischen Ansiedlung können sich unterschiedliche Bedrohungslagen ergeben. Die Ausnutzung von bekannten Schwachstellen, die über Microsoft gepatcht werden, zeigt die Bedeutung eines wirksamen Patch-Management Prozesses. Gleichzeitig bedeuten eingespielte Sicherheitsupdates nicht zwangsläufig eine vollständige Sicherheit (diese existiert ohnehin nicht), sondern es muss davon ausgegangen werden, dass Gruppierungen wie Inception Framework über Zero-Day Exploits verfügen.
Empfehlung:	Um eine möglichst hohe Resistenz gegen APTs zu erreichen, müssen verschiedene Maßnahmen in einem größeren Maßnahmenverbund wirken („Defense-in-Depth“-Strategie).
Quellen:	[1] Inception Framework: Alive and Well, and Hiding Behind Proxies