Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Technischer Bericht über den Spionagefall bei der RUAG – Zusammenfassung

Der RUAG Cyberspionagefall wurde durch das MELANI/GovCERT im Hinblick auf Aufschluss über den Angriff und weiteren Schutz analysiert. Der Bundesrat hat entschieden diesen Bericht zu veröffentlichen, damit andere Organisationen ihre Netzwerke auf ähnliche Infizierungen im Sinne der Eigenverantwortung prüfen können und um die Vorgehensweise der Tätergruppe aufzuzeigen.

Die Angreifer benutzten eine seit mehreren Jahren im Umlauf befindliche Schadsoftware der Turla-Familie. Die im Netzwerk der RUAG beobachtete Variante hat keine Rootkit-Funktionalität und setzt auf Tarnung, um unerkannt zu bleiben. Die Angreifer zeigten viel Geduld bei der Infiltration und dem weiteren Vordringen. Sie griffen nur Opfer an, an denen sie Interesse hatten, mit verschiedenen Massnahmen wie das Ausspähen von IP-Lists und extensivem Fingerprinting vor und nach der Erstinfiltration. Einmal im Netzwerk drangen sie seitwärts vor, indem sie weitere Geräte infizierten und höhere Privilegien erlangten.

Ein Hauptziel war das Active Directory zur Kontrolle weiterer Geräte und den richtigen Berechtigungen und Gruppenzugehörigkeiten für den Zugriff auf die interessanten Daten. Die Schadsoftware nutzte HTTP für den Datentransfer nach aussen mit mehreren C&C-Server-Reihen. Die C&C-Server erstellten Tasks an die infizierten Geräte. Solche Tasks können beispielsweise neue Binär- und Konfigurationsdateien oder Batchjobs sein. Im infiltrierten Netzwerk konnten die Angreifer benannte Pipes für ihre interne Kommunikation verwenden, die schwer zu entdecken sind. Es kam ein hierarchisches System zum Einsatz, bei dem nicht jedes infizierte Gerät mit den C&C-Servern kommuniziert. Einige Systeme waren sogenannte Kommunikationsdrohnen, andere Arbeiterdrohnen. Letztere kommunizierten nicht mit der Aussenwelt, sondern wurden zum Entwenden und der Weitergabe der Daten an die Kommunikationsdrohnen benutzt. Die erlangten Daten wurden durch die Kommunikationsdrohnen nach aussen transferiert. Den Schaden abzuschätzen, den die Angreifer angerichtet haben, ist schwierig und nicht Bestandteil dieses Berichts. Wir entdeckten aber interessante Muster in den Proxylogs: Phasen mit sehr geringer Aktivität sowohl bezüglich Anfragen als auch abgeführter Datenmengen abwechselnd mit sehr aktiven Perioden mit vielen Anfragen und grossen Datenmengen.

Der Bericht gibt einige Empfehlungen zu Gegenmassnahmen ab, die wir als sehr wirksam gegen diese Art der Bedrohung auf der System-, Active-Directory- und Netzwerkebene erachten.
Wichtig ist anzumerken, dass viele Gegenmassnahmen nicht kostenintensiv sind und mit vernünftigem Aufwand implementiert werden können.
Es ist zwar schwierig, eine Organisation vollständig vor solchen Tätern zu schützen; wir sind aber sicher, dass diese entdeckt werden können, da jeder Fehler macht.
Betroffene Organisationen müssen bereit sein die Spuren zu sichten und diese Informationen auszutauschen. Damit bleiben wir den Tätern dicht auf den Fersen.

Für einen Überblick über den Fall sind die Ereignisse in der untenstehenden Abbildung chronologisch dargestellt: