Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de pilotage informatique de la Confédération UPIC
Service de renseignement de la Confédération SRC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Résumé: rapport technique sur la cyberattaque contre RUAG

La cyberattaque contre RUAG a été analysée par MELANI/GovCERT à des fins d'information et de protection. Le Conseil fédéral a décidé de publier ce rapport pour permettre aux organisations de détecter la présence d'infections similaires sur leurs réseaux et mettre en lumière le mode opératoire des attaquants.

Les attaquants ont utilisé un maliciel de la famille Turla qui existe déjà depuis plusieurs années. La variante observée dans le réseau de RUAG n'a pas d'outil de dissimulation d'activité (rootkit), mais utilise du code impénétrable pour ne pas être détectée. Les attaquants ont fait preuve de beaucoup de patience pendant l'infiltration et le mouvement latéral. Ils se sont uniquement attaqués aux cibles qui les intéressaient, en recourant à diverses mesures (liste d'IP cibles et empreinte numérique complète avant et après l'infection initiale). Après avoir pénétré dans le réseau, ils ont effectué du mouvement latéral en infectant d'autres dispositifs et en obtenant des privilèges plus élevés. L'une de leurs principales cibles était l'Active Directory, qui leur permettait de contrôler d'autres appareils et d'accéder aux données qui les intéressaient en utilisant les droits et appartenances aux groupes appropriés. Le maliciel a utilisé l'HTTP pour transférer les données à l'extérieur où se trouvaient plusieurs couches de serveurs de commande et de contrôle (C&C). Les serveurs fournissaient de nouvelles tâches aux systèmes infectés. Ces tâches peuvent consister en de nouveaux codes binaires, fichiers de configuration ou travaux par lots (batch jobs). Dans le réseau infiltré, les attaquants avaient la possibilité d'utiliser pour leur communication interne des tubes nommés (named pipes) qui sont difficiles à détecter. Par ce biais, ils ont construit un système peer-to-peer hiérarchique où les dispositifs infectés ne communiquent pas tous avec les serveurs C&C. Certains de ces systèmes étaient ce que l'on appelle des drones de communication, d'autres étaient des drones de travail. Ces derniers ne communiquaient pas avec l'extérieur, mais étaient utilisés pour procéder à des vols de données, lesquelles étaient transmises aux drones de communication. Les données récoltées étaient ensuite exfiltrées par les drones de communication vers les serveurs C&C.

Il est difficile d'évaluer les dégâts faits par ces attaques, et une telle évaluation n'est pas l'objet du présent rapport. Nous avons toutefois découvert des constantes intéressantes dans les journaux proxy (proxy logs); les attaquants avaient des phases de très faible activité tant en ce qui concerne leurs requêtes que les quantités de données exfiltrées. Ces phases creuses étaient interrompues par des phases de forte activité, caractérisées par de nombreuses requêtes et d'importantes quantités de données exfiltrées.

Dans le rapport, nous émettons plusieurs recommandations et proposons des contre-mesures que nous estimons les plus efficaces contre ce type de menace au niveau des terminaux, de l'Active Directory ainsi qu'au niveau du réseau. Il est important de souligner que nombre de ces contre-mesures sont peu onéreuses et que leur mise en œuvre nécessite une charge de travail raisonnable. Même s'il est difficile d'assurer à une organisation une protection totale contre de telles attaques, nous restons persuadés que les attaquants peuvent être repérés, car ils sont aussi susceptibles de commettre des erreurs. L'organisation victime doit être capable de détecter les signes de ces attaques et d'échanger des informations à ce sujet avec des tiers afin qu'il soit possible de suivre les agissements des auteurs.

Le graphique ci-dessous présente la chronologie des événements: