# "Baldr" malware IOCs

"Baldr" is een Remote Access Tool (RAT) geschreven in Powershell. Deze malware biedt een aanvaller de mogelijkheid om stiekem commandos uit te voeren op de besmette computer.

## Werking

Baldr is een RAT client, een script dat in een permanente *loop* luistert naar de Command & Control (C2) server, en commandos uitvoert wanneer de C2 server deze aanbiedt.

Bij initiele lancering van het Baldr script, wil Baldr weten of deze al een geregistreerde ID heeft. Elke RAT creeert per computer een eigen ID, en slaat deze op in het register. Dit ID wordt bij elke request naar de C2 server meegestuurd, zodat de aanvaller de verschillende besmette computers uit elkaar kan halen.

De RAT ID wordt opgeslagen in de Register-sleutel *HKCU\SOFTWARE\Microsoft\key\SecretKey*. Als deze sleutel niet bestaat, of de waarde is leeg, dan wordt er een nieuwe ID gegenereerd door een GUID (Global Unique Identifier) aan te vragen. Deze ID wordt vervolgens opgeslagen in bovengenoemde Register-sleutel.

Na het vaststellen van de RAT ID wordt er een request gemaakt naar de C2 server op url *http://37.97.203.189:7331/ls.php?TOKEN=<token>&funx=reg&UU=<RAT ID>*. Vermoedelijk wordt met deze request de RAT geregistreerd in de C2 server.

TOKEN is een globale waarde in Baldr, die vermoedelijk gelijk is voor elke afzonderlijke RAT. Deze token wordt tijdens uitvoeren niet gewijzigd.

Na deze eerste request worden er periodiek nieuwe requests gestuurd naar de C2 server. Observatie leert dat dit veelal in 3 stappen gebeurd:

1. GET request naar *http://37.97.203.189:7331/command/<RAT ID>.cmd*
2. GET request naar *http://37.97.203.189:7331/ls.php?TOKEN=<token>&funx=uDel&filename=<RAT ID>.cmd*
3. POST request naar *http://37.97.203.189:7331/ls.php?TOKEN=<token>&funx=res&R=<RAT ID>*

De vermoedelijke flow afgaand op deze requests lijkt te zijn:

1. Maak een nieuw commando aan
2. Geef het commando aan Baldr
3. Voer het commando uit en stuur het resultaat terug naar C2

# IOCs Baldr

SHA256-hash: C32BE66E4DCC86AF71FFD8E881E92463FC4B5B79200B54EF44AC3E57ED6162F7

Register:

* Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\key

Bestandsnaam: baldr.min.ps1  
URL C2 server: 37.97.203.189:7331