G Data press release 2014

# Uroburos – Calatorie in profunzimea protectiei kernel

## Malware-ul foloseste o noua tehnologie pentru a evita protectia kernel a sistemului de operare Windows

Bucuresti (Romania) 10.03.2014

Uroburos a fost deja descris ca fiind foarte sofisticat si de mare complexitate in G Data Red Paper, document care a detaliat comportamentul malware al acestuia. Aceasta ipoteza este sustinuta din nou, de data aceasta referitor la procesul de instalare. Uroburos foloseste o tehnica nemaintalnita pana acum, pentru a ocoli Microsoft Driver Signature Enforcement, o parte esentiala a securitatii sistemului de operare.

Majoritatea programelor rootkit folosesc, de regula, modificari sau patch-uri de kernel pentru a-si ascunde activitatile si a modifica comportamentul sistemelor infectate. Microsoft a adaugat noi tehnologii la editia pe 64 bit, respectiv tehnologia Kernel Patch Protection ce verifica integritatea kernelului pentru a se asigura ca elemente importante raman nemodificate. In cazul detectarii unei modificari, este executata o functie ce are ca rezultat inchiderea sistemului prin afisarea unui ecran albastru.

Dezvoltatorii Uroburos au folosit aceleasi metode pentru a face bypass protectiei Kernel Patch, cu scopul de a evita executarea codului de bug si inchiderea sistemului.

In acelasi timp, creatorii Uroburos au utilizat o noua tehnica pentru a dezactiva Driver Signature Enforcement, exploatand o vulnerabilitate a unui driver legitim. Doar ca revocarea unei semnaturi este doar un prim pas, deoarece orice sistem care verifica o semnatura trebuie sa aiba acces la datele CRL (Certificate Revocation List). Autorii Uroburos sunt cu siguranta indeajuns de experimentati pentru a manipula procesul de verificare al sistemului de operare fara sa-l alerteze pe utilizator.

Este prima data cand expertii G Data intalnesc aceste doua tehnici de evitare a mecanismelor de protectie Windows si se asteapta ca acestea sa fie folosite si de alte programe malware in viitor.

-###-