Uroburos z Rosji

5 marca 2014

Niemiecka firma G Data SecurityLabs uważa, że za szkodliwym kodem o nazwie Uroburos stoją Rosjanie, a konkretnie któraś z rosyjskich agend rządowych. Uroburos to zaawansowany rootkit, który został stworzony nie później niż w 2011 roku.

„Uroburos to rootkit składający się z dwóch plików, drivera oraz zaszyfrowanego wirtualnego systemu plików. Jest on w stanie przejąć kontrolę nad zainfekowaną maszyną i ukryć swoją obecność. Może kraść informacje – przede wszystkim pliki – oraz przechwytywać ruch w sieci" – czytamy w ekspertyzie G Data SecurityLabs.

Uroburos pracuje z 32- i 64-bitowymi systemami Microsoftu. Działa w trybie P2P, co pozwala napastnikom na zainfekowanie maszyn w sieci wewnętrznej nawet wówczas, gdy nie mają one bezpośredniego połączenia z internetem.

„Rootkit może szpiegować każdą zainfekowaną maszynę i może wysłać napastnikom dowolne dane z komputerów ofiary. Wystarczy, że jedna z maszyn w sieci wewnętrznej ma połączenie z internetem" – stwierdzili eksperci.

Niemcy na razie nie potrafią określić dokładnego mechanizmu infekcji. Udało im się natomiast stwierdzić, że jeden z plików rootkita został skompilowany w 2011 roku, zatem Uroburos działa od co najmniej 3 lat.

Eksperci podejrzewają też, że twórcą Uroburosa jest ta sama organizacja, która w 2008 roku wykorzystała szkodliwy kod o nazwie Agent.BTZ do zaatakowania celów w USA. Uroburos sprawdza, czy dana maszyna jest zainfekowana kodem Agent.BTZ. „Jeśli zostanie on wykryty, Uroburos nie aktywuje się", informują Niemcy dodając, że zarówno w kodzie Agenta.BTZ jak i Uroburosa znajdują się rosyjskie wyrazy.

Autor: Mariusz Błoński
Na podstawie: SC Magazine
Źródło: Kopalnia Wiedzy