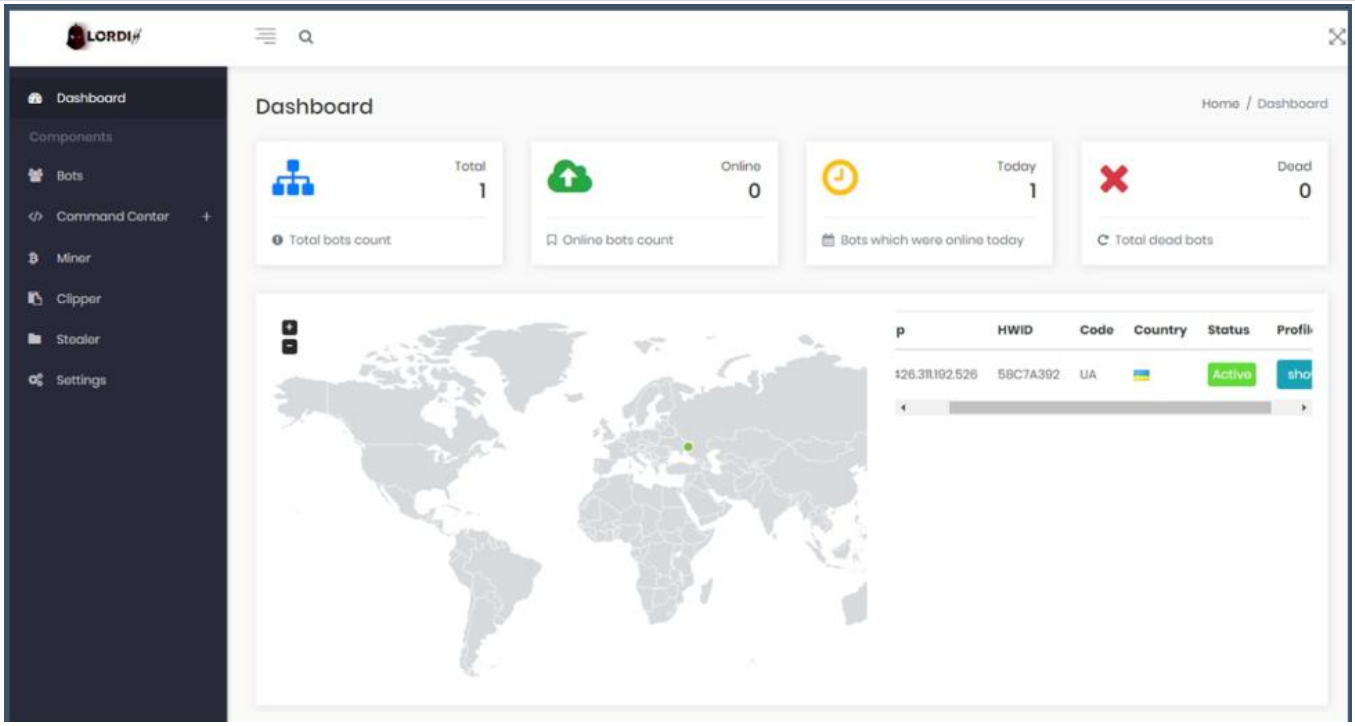
Katowice 11.12.2018

Nowy groźny wirus na horyzoncie – L0rdix

Firma Pancernik it informuje, w Dark Webie krążyć zaczął nowy i zaawansowany wirus o nazwie L0rdix. Jak donosi Ben Hunter na blogu Ensilo, wirus obecnie jest jeszcze w fazie rozwojowej, ale już można kupić jego pierwsze funkcjonalne wersje za ok. 60 dolarów (a właściwie to 4000 rubli, bo wirus ma prawdopodobnie pochodzenie rosyjskie). Wirus napisany jest w języku .NET i wykorzystuje przynajmniej dwa znane moduły maskujące – ConfuserEX i .NETGuard. Jego głównym zadaniem jest cryptomining – utajone wykorzystywanie przejętej maszyny do kopania kryptowalut. Jednak to nie wszystkie jego zadania – infekcja umożliwia wykradanie kryptowalut, a także dołącza komputer ofiary do botnetu. Pozwala także na wykradanie loginów i haseł w większości popularnych przeglądarek internetowych. Twórcy wirusa zadbali także o stosowny UI (interfejs użytkownika), który pozwala na prostą konfigurację i zarządzanie.

Tel.(32) 32 745 46 03
KRS:KRS 0000520895
REGON:243673423
NIP:634-283-09-89
SĄD REJONOWY KATOWICE-WSCHÓD, VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
Pancernik it sp. z o.o.
ul. Paderewskiego 35
40-282 Katowice
biuro@pancernik.it
www.pancernik.it



L0rdix wyposażony jest w zaawansowane funkcje wykrywania skanerów antywirusowych i środowisk wirtualnych. Od prostego podglądania procesów w command shell (procmon), po stosowanie zapytań WMI i przeszukiwania rejestru w celu zidentyfikowania maszyny wirtualnej/sandboxa. Jeśli infekcja dochodzi do skutku, wirus stara się wyłączyć silniki ochrony antywirusowej, lub je obejść, a następnie łączy się z serwerem hackerów by m. in. ściągać najnowsze aktualizacje wirusa. Wszelkie dane które zbiera w trakcie infekcji wirus zostają zaszyfrowane i wysyłane do hackerów. Dane takie umożliwiają m. in. elastyczne dobieranie momentów na utajone kopanie kryptowalut. Wirus po infekcji dba bardzo o jej utrzymanie i rozprzestrzenianie – mapuje m. in. urządzenia podłączane przez USB i je również stara się zainfekować. Dodaje się do list zadań uruchamianych przy starcie, a także replikuje się do wielu miejsc, gdzie podszywa się pod pliki i ikony (te prawdziwe ukrywa).

Na tą chwilę L0rdix wygląda na nieukończony, ale jego prosty kod i furtki jakie zostawia czynią go potencjalnie bardzo groźnym w niedalekiej przyszłości. Hakerzy co raz częściej inwestują w technologie wykrywania skanerów i ukrywania swoich wirusów. Dlatego naszym zdaniem należy przede wszystkim postawić na skuteczną ochronę pro-aktywną, wykorzystująca np. zaawansowane technologie sandboxowe, które nie dopuszczą wirusa do oryginalnych zasobów, dzięki czemu unikniemy takich infekcji jak opisywany tu L0rdix.

Źródła:
blog.pancernik.it
blog.ensilo.com