

Idea buntu znakiem nowych wirusów

Autor: Serchio
06.02.2010.

G-DATA

Odmienny od pozostałych zagrożeń czyhających w sieci nowy szkodnik Zimuse swoim działaniem nawiązuje do lat 90, kiedy to najistotniejszą rolą mechanizmów była destrukcyjna moc, a nie zysk i komercja. Niewykluczony jest również fakt, że Twórcy Zimusa chcą zdobyć uznanie wśród hermetycznie zamkniętego środowiska cybermafii.

Nowy szkodnik Win32/Zimuse znany również jako Malware.Zimuse, Worm.Win32.Zimus.a, W32/Mseus-A, Trojan.Win32.SuspectCRC poprzez destrukcję najważniejszego sektora dysku startowego uniemożliwia uruchomienie systemu operacyjnego i odczyt zapisanych na dysku informacji. Dotychczas zarejestrowano dwa warianty ("A" i "B") charakteryzujące się różnym czasem uaktywnienia mechanizmów auto-kopiowania i destrukcji startowego sektora dysku (MBR). W pierwszej fazie szkodnik wnika do systemu i rozpoczyna odliczanie czasu do ostatecznego ataku. W przypadku wariantu A wirus aktywuje się po 10 dniach obecności w systemie dla wariantu B czas uruchomienia wynosi 7 dni. Robak rozprzestrzenia się poprzez zewnętrzne pamięci USB oraz sieć internet (strony www, programy P2P, e-mail).

Użytkownicy zaopatrzeni w programy firmy G Data dzięki dwóm niezależnym skanerom oraz codziennym aktualizacją pozostają bezpieczni. Zimuse przy próbie wnikięcia do systemu ofiary, jest rozpoznawany jako wirus Dropped:Worm.Zimuse.A, oraz Win32:Zimuse-B.

Usunięcie Zimusa z zainfekowanego systemu, będzie wymagać użycia odpowiednio przygotowanych programów oraz dodatkowej pracy użytkownika. Dodatkowo Laboratorium G Data informuje, że w związku z ingerencją Zimusa w sektor startowy dysku, standardowe formatowanie partycji "c:" nie rozwiąże problemu. Aby zlikwidować wirusa konieczne jest zatrzymanie jego usług, usunięcie ciała oraz repozytorium. Kolejny krok to odnowienie głównego rekordu rozruchowego (MBR) za pomocą płyty instalacyjnej systemu Windows:

Instrukcje odnowienia rekordu rozruchowego MBR dla Windows Vista:

1. Proszę zainicjować instalację systemu
2. Umieść dysk instalacyjny systemu Windows Vista w napędzie i uruchomić ponownie komputer
3. Wszystkie dalsze wskazane czynności wykonaj podczas jednej sesji tzn. bez restartowania komputera
4. Gdy pojawi się okno wybór języka, czasu, waluty, klawiatury - kliknąć przycisk Dalej
5. Wybrać opcję „Napraw komputer”
6. Kliknąć nazwę systemu operacyjnego i następnie wybrać opcję Dalej
7. W oknie dialogowym Opcje odzyskiwania systemu - kliknij polecenie „Wiersz polecenia”
8. Wpisz bootrec.exe /fixmbr a następnie naciśnij klawisz ENTER.
9. Zamknij okno wiersza polecenia i uruchom system ponownie

Instrukcje odnowienia rekordu rozruchowego MBR dla Windows XP:

1. Proszę zainicjować instalację systemu
2. Umieść dysk instalacyjny systemu Windows XP w napędzie i uruchom ponownie komputer
3. Wszystkie dalsze wskazane czynności wykonaj podczas jednej sesji tzn. bez restartowania komputera
4. W programie instalacyjnym wybierz naprawę instalacji systemu, naciskając literę R
5. Kolejną opcją jest pole wyboru systemu, gdzie najczęściej widoczna jest wartość 1: C:\WINDOWS – (naciśnij 1 i potwierdź ENTEREM)
6. Po pojawieniu się wiersza C:\WINDOWS> …dopisz fixmbr czyli C:\WINDOWS>fixmbr i (potwierdź ENTEREM)
7. Po pojawieniu się pytania „Czy na pewno chcesz zapisać nowy rekord MBR?” naciśnij literę „t” (potwierdzając ENTEREM)
8. W C:\WINDOWS> wpisz exit czyli C:\WINDOWS>exit (potwierdzając ENTEREM)