Na przełomie kwietnia i maja obserwowaliśmy duży 80% przyrost komputerów zombie. Tym samym cyberprzestępcom z poziomu 8 mln udało się wskoczyć na pułap 15 mln zainfekowanych aktywnych maszyn. Największy odsetek zarażonych komputerów należy do naszych sąsiadów z zachodniej granicy i mieszkańców Indii. Obecna fala infekcji nadal rośnie i niesie ze sobą wysokie ryzyko przedostania się groźnych plików do systemu ofiary.

Zombie to zainfekowany komputer, wykorzystywany przez cyberprzestępców jako narzędzie do rozpowszechniania infekcji. Dzięki komunikacji pomiędzy napastnikiem a szkodliwym programem wstrzykniętym do systemu ofiary, cyberprzestępcy mają możliwość wydawania konkretnych poleceń ataku. Obecnie tak duży przyrost zombie pozwoli spamerom wygenerować miliony niepożądanych wiadomości email. Możemy spodziewać się nowej fali spamu zawierającego wiadomości wykorzystujące aktualne tematy zachęcające do kliknięcia w niebezpieczne linki oraz fałszywe oferty biur podróży lub zakupu najnowszego sprzętu za przysłowiową złotówkę.

Łukasz Nowatkowski z firmy G Data Software - producenta oprogramowania antywirusowego i szyfrującego dane. „15 mln komputerów skojarzonych ze sobą dzięki sieci botnet jest źródłem toksyn dla wszystkich użytkowników sieci. Przed nami walka z kolejnymi próbami destabilizacji pracy systemów komputerowych, masowej wysyłki spamu oraz infekcji niezabezpieczonych stacji roboczych. Za przyczynę tak wysokiego poziomu odpowiedzialni są użytkownicy bagatelizujący zagrożenia czyhające w sieci Internet. Nieświadomi infekcji własnego komputera stanowią niebezpieczeństwo nie tylko dla samych siebie, ale i dla pozostałych użytkowników sieci.”

Eksperci z firm antywirusowych obawiają się również efektów zamieszania związanego z KHOBE. Ujawnienie nowej luki systemu Windows może pociągnąć za sobą spore konsekwencje w niedalekiej przyszłości. Z całą pewnością znajdą się bowiem ludzie chętni wykorzystać nowe możliwości ataku. Większość producentów programów antywirusowych w chwili obecnej musi wykonać duże poprawki w swoich rozwiązaniach. Dotyczy to prawie wszystkich pakietów Internet Security, ESET Smart Security 4.2.35.3, Kaspersky Internet Security 2010, Avast! Internet Security, Panda Internet Security 2010 i wielu innych popularnych do tej pory programów. Niestety wciąż niewiadomo kiedy to nastąpi.

Eksperci z **G Data Software** komentując problem luki słusznie nawiązują do sytuacji, kiedy to z powodu uodpornienia się jednej bakterii na mydło przestajemy myć ręce przed jedzeniem. Dobrze wiemy do czego doprowadziłaby taka sytuacja. „Luka jest poważna jednak znana nam od dłuższego czasu. Wykorzystanie jej wymaga szeregu działań, które bez problemu wyłapać może większość z aplikacji wymanionych w raporcie organizacji matousec” – dodaje Nowatkowski

Zapobieganie obecności szkodliwych programów w systemie komputera to ciągły proces przeciwdziałania hakerskim atakom. Aktualizacje systemu oraz stosowanie programów antywirusowych minimalizuje ryzyko infekcji. Dodatkowo użytkownicy komputerów podczas surfowania w sieci powinni pamiętać o zachowaniu ostrożności oraz rozsądku. Programy antywirusowe obecnie powinny stanowić integralną część każdego systemu.

G Data Software