**Czym jest Slammer?**

Slammer nazywany również Sapphire lub SQLExp to robak czyli samoreplikujący (nie potrzebuje nosiciela [pliku] który może być uruchomiony bezpośrednio w środowisku operacyjnym ) się program komputerowy, który  rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym lub naiwności użytkownika. Ten robak był prostym fragmentem kodu, który ukierunkowano na server sql, , kod robaka to zaledwie **376 bajtów**, generuje on w nim losowe adresy IP (potrzebne do rozprzestrzeniania się) oraz jeden pakiet UDP (wielkości 404 bajtów). Slammer był najszybciej rozwijającym się robakiem swoich czasów.

**UDP** – protokół pakietów użytkownika – jeden z [protokołów internetowych](https://pl.wikipedia.org/wiki/Protoko%C5%82y_internetowe). Jest to protokół bezpołączeniowy, więc nie ma narzutu na nawiązywanie połączenia i śledzenie. Nie ma też mechanizmów kontroli przepływu i retransmisji. Korzyścią płynącą z takiego uproszczenia budowy jest szybsza [transmisja](https://pl.wikipedia.org/wiki/Transmisja) danych i brak dodatkowych zadań, którymi musi zajmować się host posługujący się tym protokołem.

#robaki mogą również wysyłać emaile z poczty luz niszczyc pliki.

**Jak wyglądała infekcja?**

Robak wykorzystuje lukę w oprogramowaniu Microsoft Server 2000 i wysyła pakiet o wielkości 376 bajtów na port UDP 1434 tegoż serwera. Po jego zainfekowaniu (błąd przepełnienia bufora), Slammer zaczyna wysyłać ogromne ilości pakietów i kodu robaka na losowe adresy IP, przez co powoduje spowolnienie lub zablokowanie serwera, na szczęście nic nie wskazuje na to, że robak niszczy dane przechowywane w zainfekowanych systemach.

#Robak na zainfekowanym komputerze wysyłał datagram UPD do portu 1434. Datagram wykorzystywał lukę w zabezpieczeniach SQL Server Monitor, dotyczącą przepełnienia bufora na stosie i wykorzystywał resztę exploita (czyli [program](https://pl.wikipedia.org/wiki/Program_komputerowy) mający na celu wykorzystanie istniejących [błędów](https://pl.wikipedia.org/wiki/B%C5%82%C4%85d_(informatyka)) w oprogramowaniu.). Gdy znajdzie się w pamięci celu, zaczyna wysyłać datagramy swojego exploita i kodu robaka na losowe adresy IP w celu zainfekowania nowych celów.

**#Exploit** – [program](https://pl.wikipedia.org/wiki/Program_komputerowy) mający na celu wykorzystanie istniejących [błędów](https://pl.wikipedia.org/wiki/B%C5%82%C4%85d_(informatyka)) w oprogramowaniu.

#Exploit wykorzystuje występujący w oprogramowaniu błąd programistyczny w celu przejęcia kontroli nad działaniem procesu i wykonania odpowiednio spreparowanego [kodu maszynowego](https://pl.wikipedia.org/wiki/J%C4%99zyk_maszynowy) , który najczęściej wykonuje [wywołanie systemowe](https://pl.wikipedia.org/wiki/Wywo%C5%82anie_systemowe) uruchamiające [powłokę systemową](https://pl.wikipedia.org/wiki/Pow%C5%82oka_systemowa) z uprawnieniami programu, w którym wykryto lukę w zabezpieczeniach.

**Kiedy i co było jego celem?**

Po raz pierwszy robak pojawił się 25 stycznia 2003 roku o godzinie 6:00.

W Stanach Zjednoczonych serwery aktywacyjne systemu Windows XP w stanie Waszyngton zostały wyłączone.

Continental Airlines korzystało z długopisów i papieru, aby rejestrować rezerwacje i bilety. Linia lotnicza musiała opóźnić i odwołać niektóre loty, choć żadne opóźnienia nie trwały dłużej niż 30 minut.

Banki w USA i Kanadzie zostały mocno dotknięte. Większość bankomatów Bank of America stała się bezużyteczna i chociaż większość z nich działała do wieczora, niektórzy klienci zgłosili, że nie byli w stanie dobrze wykorzystać ich do następnego dnia. Bankomaty Washington Mutual i inne usługi bankowe były niedostępne przez większą część dnia. Klienci kanadyjskiego Imperial Bank of Commerce w Toronto nie byli w stanie wypłacić pieniędzy za pomocą bankomatów.

Awaryjna sieć 911 w Seattle nie działała przez pewien czas.

Sieć komputerowa Atlanta Journal-Constitution została zainfekowana, zmuszając gazetę do opóźnienia publikacji pierwszego niedzielnego wydania i opóźniając aktualizacje strony internetowej gazety.

Również Korea Południowa została dotknięta. Niektóre koreańskie media twierdziły, że cała infrastruktura internetowa została zniszczona i utracili miliardy. Klienci SK Telecom utracili połączenia internetowe.

W Portugalii ponad 300 000 klientów Cable ISP Netcabo utraciło dostęp do Internetu.

Elektrownia nuklearna w Ohio również została zaatakowana – i to nawet mimo tego, że cała sieć chroniona była przez firewall.

Slammer rozprzestrzenił się na ponad 90 procent wszystkich podatnych na atak hostów w ciągu 10 minut i zainfekował łącznie około 359 000 komputerów. Jego czas podwojenia populacji wynosił około 37 minut. 5 z 13 głównych serwerów DNS w Internecie uległo awarii, a około 10 z nich doświadczyło ogromnej utraty pakietów z powodu przepustowości zużywanej przez robaka.

#Londyńska firma wywiadu rynkowego powiedziała, że ​​robak spowodował utratę produktywności między 950 a 1,2 miliarda dolarów w ciągu pierwszych pięciu dni na całym świecie.

**Szybkość infekowania:**

W pierwszej minucie swojego działania robak podwajał ilość zainfekowanych komputerów co ok. 8.5 sekundy, po trzech minutach ilość skanowanych przez kopie robaka maszyn wyniosła ok. 55 milionów / sekundę.

Robak zainfekował 75 tys serwerów w 10 min i cały czas się rozprzestrzeniał.

Zanim producenci oprogramowania antywirusowego stworzyli odpowiednie łatki, Slammer zdążył zainfekować ponad 1 milion serwerów i internet na moment przestał działać, co spowodowało ponad miliard dolarów strat.. A cały koszt Slammera przerósł nawet 1 bilion USD.

**Co ciekawe:**

Już w lipcu 2002 roku wykorzystywana przez robaka luka w oprogramowaniu została dostrzeżona i uwzględniona w poprawce oraz kolejnych uaktualnieniach, jednak wiele organizacji jej jeszcze nie zastosowało. (Michael Baracella)

Oryginalny kod robaka zawierał błąd w generatorze liczb losowych, który spowodował, że niektóre maszyny nie zostały nigdy przeskanowane, ponieważ ich adresy nie mogły być wygenerowane przez żadną kopię Slammera.

**Kilka lat później:**

W 2011 roku Slammer nagle zniknął i myślano, że już się nie pojawi

Między 28 listopada a 4 grudnia 2016 r. Robak Slammer znów się pojawił. Pochodził z adresów IP w Chinach, Meksyku, Ukrainie i Wietnamie, a niewielka ich część pochodziła z Rosji, Wenezueli, Argentyny, Tajlandii i Stanów Zjednoczonych. (Maszyny w stanach)

**Kto jest za to odpowiedzialny?**

Istnieje możliwość, ze za rozpowszechnienie robaka odpowiada **Benny** – czeski koder wirusów, który jest obecnie pracownikiem firmy zajmującym się oprogramowaniem antywirusowym Zoner Antivirus, jednak nie udowodniono, że kiedykolwiek jakiś z jego wirusów lub robaków został przez niego wydany.