Fot. Nick Benjaminsz

Gadu-Gadu może się okazać skutecznym „wytrychem" pozwalającym na dostęp do skrzętnie chronionych danych – uważają informatycy z Poznańskiego Centrum Superkomputerowo – Sieciowego.

Dariusz Kaczyński, MON

Małe słoneczko – ogromna dziura

Gadu-Gadu, program napisany przez Łukasza Foltyna, dystrybuowany przez spółkę sms-express.com zrobił w Polsce zawrotną karierę. Używa go miesięcznie około 3 milionów osób, jest zainstalowany na wielu, jeśli nie większości podłączonych do Internetu komputerach. Nie tylko domowych, ale także pracujących w sieciach korporacyjnych, po których krążą niekiedy bardzo wrażliwe i cenne dane. Korzystanie z tego programu jest tyleż powszechne, co tolerowane przez pracodawców i administratorów sieci. Może się ono jednak okazać zaskakująco niebezpieczne.

Informatycy z Poznańskiego Centrum Superkomputerowo – Sieciowego znaleźli w programie aż siedem różnego rodzaju dziur.

– Od zmian w obsłudze wiadomości, która, na przykład, zamiast do adresata dociera do nieznajomej osoby, po luki umożliwiające uruchomienie kodu (także złośliwego!) na komputerze klienta – wymienia Błażej Miga.

– Luki umożliwiają też kradzież dowolnych plików z komputera klienta – dodaje Jarosław Sajko.

Co gorsza, użytkownik nie jest w żaden sposób informowany o tym, co dzieje się na jego twardym dysku. Po prostu pliki nagle znikają. Włamywacz może też zrobić coś wręcz przeciwnego – podrzucić delikwentowi dowolny plik, zapisując go na dysku ofiary.

Można wejść przez lufcik

Ten niewielki program może stworzyć ogromny wyłom w dobrze zabezpieczonej sieci. Włamywacz atakuje komputer pracownika, przez dziurę w GG, a na serwer firmy, gdzie są interesujące go dane, łatwo wchodzi podszywając się pod uprawnionego użytkownika. Zabezpieczenia serwera nie mają wtedy podstaw, by się włączyć.

Poznańscy informatycy opracowali w warunkach laboratoryjnych narzędzia, które z wykorzystaniem dziur w GG pozwalają dokonywać opisanych włamań. Złą dla użytkowników komunikatora wiadomością jest to, że narzędzia te działają, tak jak założyli sobie ich projektanci.

Niebezpieczne metamorfozy

Błędy w GG pozwalają na atak najbardziej bezczelny: na podszycie się pod użytkownika. Ktoś odpowiadając na wiadomość od znajomego z listy kontaktów tak naprawdę otwierał intruzowi furtkę do swojego komputera.

– By temu skutecznie zapobiec, musielibyśmy nie tylko ignorować wiadomości od nieznajomych, ale też usunąć wszystkich z listy kontaktów – uświadamia Miga. *– Bo wystarczy kliknąć na kopertę u dołu ekranu sygnalizującą nową wiadomość, a złośliwy kod już może być wykonany na komputerze. Z kolei, gdy przestaniemy sprawdzać, czytać wiadomości, program straci wszelką funkcjonalność.*

Informatycy podkreślają, że o ile to oni oficjalnie ujawnili błędy, trudno ocenić, ilu użytkowników wiedziało o nich wcześniej i po cichu zabawiało się – choćby tylko wymianą numerów UIN, ale równie w znacznie bardziej niebezpieczny sposób. Informatycy przestrzegają przed zaufaniem do automatycznej instalacji nowych wersji programu: od jakiegoś czasu nie działa. Być może, mechanizm ten producent celowo wyłączył, bo też był dziurawy. Przestrzegają, że lista dziur w GG nie musi być zamknięta. W ostatnich dniach wykryli kolejne dwie.

Program jak zamek

Mało kto ma już wątpliwości, że istnieje zamek odporny na włamanie. Zwykle wie jednak, że opłaca się utrudnić złodziejowi jego proceder – stosując zabezpieczenia nietypowe, łączyć jedne z drugimi, a przestarzałe wymieniać. W informatyce, gdzie postęp jest błyskawiczny, to ostatnie jest szczególnie ważne. Podobnie jak w przypadku zamków, włamywacze szczególnie interesują się aplikacjami typowymi, stosowanymi powszechnie – jak Gadu Gadu, czy rodzina Microsoft Windows. Wysiłek musi się opłacić – raz opracowane narzędzie musi pozwolić wiele razy się obłowić. Nie opłaca się budować „wytrycha" do zamka stosowanego rzadko.

Niech użytkownik wie, że nie należy złodziejowi ułatwiać pracy – stwarzać pokusy – począwszy od publikowania nierozważnie w sieci prawdziwego adresu mailowego, czy trzymania na słabo zabezpieczonych dyskach cennych danych. O tym, jak niebezpieczny może być zwykły adres e-mail podany do publicznej wiadomości można się przekonać, gdy dostaje się pocztę od Błażeja Migi. Listy są podpisane cyfrowo, co gwarantuje, że treść poczty nie zmieniła się po drodze od nadawcy. W skali kraju wciąż jest to ogromną rzadkością.

Fot. Gail Kewney

Ciemne zaułki cyberprzestrzeni

Coraz częściej pojawiają się plotki, że producenci oprogramowania sami przymykają oko na dziury, by w stosownym czasie zarobić na aktualizacji. Można o tym dyskutować, pewne jest natomiast, że dziury są wynikiem pośpiechu wynikającego z praw rynku. Terminy premier nie tolerują opóźnień w pracy nad programami.
– *Stąd duże prawdopodobieństwo, że popularna, komercyjna aplikacja na której premierę wszyscy czekają, będzie mieć sporo dziur* – podkreśla Sajko.

Admin czy audyt

Łudzą się ci, który sądzą że wystarczy zabrać pracownikom możliwość instalowania aplikacji. Firma sms-express, producent GG przygotowuje wersję do uruchamiania przez stronę WWW. A we współczesnej firmie nie sposób zabronić pracownikom korzystanie z witryn internetowych – to zupełnie sparaliżowałoby ich pracę.

Poznańscy informatycy podkreślają, że Gadu Gadu nie ma audytu bezpieczeństwa. Tam, gdzie przykłada się wagę do bezpieczeństwa, aplikacje taki audyt mają. Zespoły specjalistów testują program, znęcają się nad nim na wszelkie sposoby, wyszukując dziury – a wszak GG jest produktem komercyjnym.
– *My nawet nie mieliśmy dostępu do kodu źródłowego aplikacji, a to tam powinno się szukać błędów* – podkreśla Sajko.

Zdaniem Krzysztofa Szalwy – członka zarządu spółki sms-express.com, której własnością jest Gadu-Gadu oczekiwanie udostępnienia informatykom spoza spółki kodu źródłowego programu to żądanie wygórowane.
– *Rzeczywiście to program komercyjny, a więc jego kod źródłowy ma wartość rynkową. Siłą faktu, więc chcemy zapobiec przedostaniu się go w ręce konkurencji, choćby za pośrednictwem audytora* – twierdzi. – *Trzeba też pamiętać, że taki audyt jest kosztowny, a nasz program dynamicznie się zmienia. Trudno wyobrazić sobie jak miałoby sprawdzanie bezpieczeństwa wyglądać w praktyce.*

Czy firmy przeprowadzające audyty bezpieczeństwa nie gwarantują zachowania tajemnicy?
– *Różnie z tym bywa* – twierdzi Szalwa – *Zasada jest prosta – im firma pewniejsza tym audyt droższy. A w naszym przypadku o jednym trudno mówić.*

Dlaczego? Bo wersja GG zmienia się raz na kilka miesięcy. Od fazy sms-express – prostego programu służącego do wysyłania smsów, do obecnej formy Gadu Gadu przeszło całkowitą metamorfozę, choć odbywała się ona ewolucyjnie.

– *Nasz sukces opiera się na oferowaniu przeciętnemu użytkownikowi Internetu komunikatora, który zawiera tylko to, czego on potrzebuje. Poszczególne funkcje dodajemy bardzo ostrożnie, ale jednak to robimy. Nawet, jeśli zdecydowalibyśmy się na audyt – jego wynik byłby miarodajny do następnej aktualizacji. A co później? Kolejny?* – zastanawia się Szalwa.

Jego zdaniem i to, że program podbił rynek, i to, że nie traci popularności wśród internautów zasadza się na wyczuciu chwili.
– *Przyglądamy się, które funkcje – potencjalnie możliwe do włączenia do programu upowszechniają się w Sieci. Decydujemy się je dodać, gdy uznamy, że przeciętna większość ich potrzebuje* – mówi. – *Teoretycznie, gdy prześpimy jakiś moment możemy stracić część użytkowników na rzecz konkurencji.*

– *W żadnym stopniu nie lekceważymy sprawy bezpieczeństwa. Gdy tylko dowiedzieliśmy się o lukach natychmiast je naprawiliśmy* – mówi Szalwa. – *Ale nie demonizowałbym sprawy. Nie ma programów absolutnie bezpiecznych. Czego dowodzi fakt, że znacznie więksi od nas miewają z tym problemy.*

Poznań górą!

Poznańskie Centrum Superkomputerowo Sieciowe wyrasta dziś w kraju na ceniony ośrodek informatyki, znany m. in. z prac nad zabezpieczeniami i ważnych odkryć. Dwa miesiące wcześniej Adam Gowdiak z PCSS wykrył luki w oprogramowaniu Java, powszechnie stosowanym w telefonach komórkowych. Chodzi o dziury umożliwiające osobie z zewnątrz przejęcie kontroli nad wybranym telefonem. Nieco wcześniej informatycy z PCSS wykryli cały szereg błędów w systemie operacyjnym Windows Microsoftu.