

Cyberoszuści wciąż atakują, tym razem ofiarą padł najczęściej instalowany w Polsce komunikator Gadu-Gadu 10. W dniu wczorajszym specjaliści firmy CORE, dystrybutora oprogramowania antywirusowego AVG Technologies wpadli na trop nielegalnego instalatora najbardziej popularnego polskiego komunikatora. Ofiarą naciągaczy mogło paść nawet parę tysięcy nieświadomych zagrożenia użytkowników internetu.

Działalność cyberprzestępców, oszustów oraz zwyczajnych e-naciągaczy nie zna granic, przekonaliśmy się o tym kolejny raz w dniu wczorajszym. Za cel ataku została obrana tym razem polska aplikacja Gadu-Gadu 10, przestępcy umieścili w sieci fałszywą wersję instalatora programu, będącą wręcz książkowym przykładem phishingu – czyli elektronicznego wyłudzenia pieniędzy.

Podejrzany plik instalacyjny **Gadu-Gadu** przesłaliśmy do centrali **AVG Technologies**, dzisiaj w godzinach porannych nasze podejrzenia się potwierdziły – mówi Arkadiusz Zakrzewski, Specjalista pomocy technicznej AVG.PL. Samo wyłudzenie to jeszcze nie koniec atrakcji wraz z utratą gotówki otrzymujemy infekcję komputera gratis. Fałszywy plik instalacyjny Gadu-Gadu został zainfekowany nową odmianą konia trojańskiego Downloader.Generic.BLSS. Aktualizacja baz wirusów AVG została już przeprowadzona i nowa odmiana jest już wykrywana w bazie sygnatur AVG - dodaje.

Jak przyznaje Pan Arkadiusz u niedoświadczonego użytkownika fałszywy instalator może nie wywołać podejrzeń, jest napisany poprawnie i opatrzony logo aplikacji, której się spodziewamy. Podstawowa różnica tkwi w tym, że oryginalne Gadu-Gadu jest narzędziem bezpłatnym, a plik instalacyjny, który został wykryty w sieci żądał wysłania dwóch smsów na numer Premium (7,32zł brutto) zarejestrowany w Chile, w celu dokończenia instalacji. Celem smsa jest niestety tylko i wyłącznie wyłudzenie od nas pieniędzy.

W pierwszej wiadomości odpowiedzi otrzymujemy informację, że jeszcze tylko jeden sms dzieli nas od otrzymania naszego kodu. Po wysłaniu ponownego smsa otrzymujemy sześciocyfrowy kod do instalacji Gadu-Gadu 10. Kod jest sprawdzany online i połączenie jest nawiązywane przez proces instalatora z adresem IP 195.78.228.246:80. Pod tym adresem znajduje się strona zarejestrowana w hiszpańskiej Sewilli.

Jest to panel operatora firmy świadczącej usługi płatności smsem. W przypadku prób wprowadzenia fałszywego kodu program wyświetla komunikat, że podany kod jest nieprawidłowy. Jeśli spróbujemy instalacji bez aktywnego połączenia z Internetem lub zablokujemy proces instalatora zaporą to ujrzymy komunikat:

Tu już widać problemy z tłumaczeniem – brak polskich znaków, tylko jeden wyraz zawiera jakby przypadkowo wprowadzoną literkę „ó”. Ewidentnie ktoś się nie przyłożył do tłumaczenia okienek komunikatów. Dlaczego do tłumaczenia? Po wydobyciu plików źródłowych specjaliści firmy CORE znaleźli obcojęzyczną grafikę:

Ktoś odpowiedzialny za stworzenie polskiej wersji oszustwa nie przyłożył się do posprzątania po oryginalnej wersji. W oryginale wyłudzone były pieniądze na koszt instalacji Windows Live Messenger w Hiszpanii, Chile, Argentynie, Ekwadorze wnioskując z ikon flag umieszczonych obok opisu procedury – również 2 smsy o określonej treści tylko na inny numer usługi Premium.

W stopce instalatora na etapie wprowadzenia kodu otrzymanego w odpowiedzi na dwa smsy widzimy adres strony www.libelasms.com – to zarejestrowany w Chile operator sieci komórkowej. Po podaniu poprawnego kodu instalacyjnego w oknie fałszywego instalatora ten kończy pracę uruchamiając prawdziwy instalator komunikatora Gadu Gadu 10.

Oszustwo jest dość proste i szyte grubymi nićmi niestety osoby niedoświadczone mogą paść ofiarą i stracić nieco ponad 14zł, przy okazji infekując swój system nową odmianą konia trojańskiego.

Zastanawiające są poprawne treści smsów otrzymywanych z numeru Premium oraz wymóg współpracy z polskimi operatorami sieci komórkowych.

Sprawa jest analizowana przy współpracy ze wsparciem technicznym komunikatora Gadu Gadu, która tak jak i firmy CORE i AVG przestrzega przed oszukańczą wersją i przypomina, że oryginalne Gadu-Gadu 10 jest udostępnione bezpłatnie tylko i wyłącznie na stronie www.komunikator.gadu-gadu.pl.

Szczegółowe informacje wraz z zrzutami ekranowymi dostępne są na www.techblog.avg.pl

Przedsiębiorstwo Informatyczne CORE