Urząd Gminy
Radziechowy-Wieprz

Urząd Gminy Radziechowy-Wieprz
34-381 Radziechowy, Wieprz 700
tel. 33 867 66 10, fax. 33 867 66 13
e-mail: ug@radziechowy-wieprz.pl
www.radziechowy-wieprz.pl

Kolejna fala fałszywych faktur... - czyli uwaga na wirusy komputerowe!

Maile przypominają oczywiście wiadomości, jakie zwykle otrzymują klienci czy abonenci danej firmy, z tym że trafiają one także do osób z danymi firmami niezwiązanych. Podszywając się pod Allegro przestępcy rozsyłają między innymi złośliwe oprogramowanie, spakowane w archiwum ZIP, podobnie jak miało to miejsce w mailach udających faktury UPC. Ciekawszą formą ataku jest jednak wiadomość łudząco podobna do tej, jaką otrzymują użytkownicy portalu aukcyjnego, jeśli nie dokonają wpłaty na czas. Od oryginalnej (po lewej) różni się między innymi brakiem odnośnika do informacji o wpłacie, brakiem imienia użytkownika i oczywiście numerem konta bankowego – to po prawej bynajmniej do PayU nie należy i pod żadnym pozorem nie należy przelewać na nie pieniędzy.

Pomysłowo przestępcy rozsyłają także wiadomości udające faktury od T-Mobile. Tradycyjnie, w załączniku znajduje się szkodnik. T-Mobile zapewnia, że nie ma z tą korespondencją nic wspólnego i podejmie wszelkie możliwe kroki, aby ten proceder ukrócić.

W wiadomościach podszywających się pod informację o odebraniu paczki z paczkomatu InPost oszuści zdecydowali się zagnieździć także piosenkę (z niej pochodzi cytat „ze słońcem twarzą w twarz”). Poza tym tu również znalazło się archiwum ze szkodliwym plikiem.

Do grona operatorów, pod których podszywają się niegodziwe osoby, dołączyła Netia. W wiadomości znajdzie się kwota do zapłaty, numer faktury i numer konta bankowego, nie będzie jednak danych klienta, a numer abonencki będzie wygenerowany losowo. Z rozsyłanego pocztą elektroniczną oświadczenia Netii w tej sprawie możemy dowiedzieć się, że celem atakujących jest uzyskanie danych bankowości elektronicznej kilku banków. Służyć temu ma zaszyty w fałszywej fakturze trojan. Warto zaznaczyć, że nie jest to pierwsza fala takich ataków. Niedawno operator informował, że szkodliwe wiadomości były rozsyłane z Rosji. Netia prosi o ignorowanie tych wiadomości, mimo że są dostarczane z adresu w domenie `netiaonline.pl`.

Bardzo proste, ale nie mniej szkodliwe wiadomości, rozsyłane są z domen Orange.com. Tu znów trzeba uważać na spakowany załącznik. Poczta Polska z kolei informuje o możliwości odebrania przesyłki za pobraniem.

W obliczu tak licznych ostatnio ataków zalecamy szczególną ostrożność.

Najlepiej nie otwierać załączników, a wezwania do zapłaty weryfikować w centrum obsługi klienta danej firmy.

Źródło: dobreprogramy.pl