Hakerska sztuczka **na paczkę**

Internetowi oszuści szukają coraz wymyślniejszych sposobów, by wyłudzić pieniądze. Tym razem postanowili rozsyłać fikcyjne zawiadomienia o nieodebranej przesyłce. Wykorzystali do tego logotypy m.in. Poczty Polskiej oraz firmy kurierskiej DHL. Naiwność kończyła się dla odbiorcy korespondencji dość przykro – komputer całkowicie blokowano, a za odzyskanie własnych plików trzeba było zapłacić. Mimo, iż firmy wydały oświadczenia i cały czas przestrzegają przed oszustami, a sprawa stała się dość głośna, hakerzy nie ustają w poszukiwaniu ofiar.

Leszek Pogorzelski

Mechanizm oszustwa nie jest szczególnie wyrafinowany, przez co dość łatwo odkryć mistyfikację. Mimo to wiele osób pada ofiarą hakerów. List opatrzony dobrze znanym znakiem Poczty Polskiej lub firmy kurierskiej informuje o awizowanej przesyłce. W przypadku poczty pojawia się informacja, że przesyłkę trzeba odebrać możliwie szybko, bowiem każdy dzień opóźnienia skutkuje naliczeniem 50 zł opłaty. Aby odebrać przesyłkę należy wydrukować awizo, które znajduje się pod załączonym linkiem. Link ten uruchamia procedurę pobrania skompresowanego pliku .zip, który po rozpakowaniu infekuje komputer. W przypadku listów „od firmy kurierskiej" plik zamieszczany jest jako załącznik. Co ciekawe, w korespondencji nie ma adresu, pod którym rzeczona paczka miałaby oczekiwać na odbiorcę, co powodowało dodatkową motywację, by przejrzeć załączniki i dowiedzieć się czegoś więcej. Uaktywniony załącznik natychmiast instaluje na dysku plik ransomware, który szyfruje dysk i blokuje dostęp do całej jego zawartości. Następnie na ekranie pojawia się komunikat z informacją o okupie. Aby odzyskać pliki, ofiara ataku musi uiścić opłatę w walucie elektronicznej bitcoin.

Dotychczas eksperci wyodrębnili dwa główne wirusy, które odpowiadają za blokowanie komputera. Pierwszy z nich – Infostealer. Banker.C – przejmuje i przekazuje do swojego „właściciela" sekwencje znaków wciskanych na klawiaturze użytkownika. W ten sposób haker może uzyskać dostęp do loginów i haseł ofiary, np. tych używanych w bankowości internetowej. Poza tym wirus spowalnia działanie systemu, często też komputer nagle się wyłącza. Drugi z kolei – CryptoLocker – szyfruje dostęp do danych na dysku. W obu przypadkach na ekranie zawirusowanego komputera pojawia się komunikat z żądaniem dokonania opłaty.

Aby uchronić się przed atakiem należy przede wszystkim dbać o aktualność swoich programów antywirusowych i ich baz danych. Z drugiej strony – nie należy polegać na nich bezwzględnie i z dużą podejrzliwością podchodzić do wszystkich informacji, których nie oczekiwaliśmy. Większość ekspertów zaleca, by w przypadku wątpliwości, nie korzystać z lików czy załączników, ale wpisać numer rzekomej przesyłki bezpośrednio na stronie poczty lub firmy kurierskiej. To najskuteczniejszy sposób weryfikacji informacji o przesyłce. Aby zabezpieczyć się przed utratą cennych danych, warto także regularnie wykonywać kopię zapasową swoich plików. I – co bardzo ważne – dysku zewnętrznego, na którym przetrzymujemy zarchiwizowane dane, nie podłączać na stałe do komputera, bowiem aplikacje blokujące są w stanie zainfekować wszystkie dostępne dyski.

Na szczęście nasz kraj nie jest głównym celem ataku internetowych oszustów. Według raportu „TorrentLocker. Ransomware in a country near you", wydanego przez firmę Eset, fałszywe listy najczęściej pojawiają się w Australii, Turcji, Włoszech, Czechach, Wielkiej Brytanii i Holandii. Tylko w ubiegłym roku hakerom udało się zainfekować w tych krajach 39,7 tys. komputerów. Co ciekawe, zaledwie 570 osób (1,45 proc.) zdecydowało się zapłacić oszustom za odzyskanie dostępu do danych. Cena, jaką musieli zapłacić, wynosiła od 300 do 600 dolarów wypłacanych w bitcoinach. ■

(współpraca SBW)

Fot: fotolia.com

Od DHL Logistik <as@escgrup.com>
Temat **Sledzenie dostawy przesylki DHL**
Do Sławomir Dolecki

Sledzenie trasy przesylki DHL

DHL Sendungsverfolgung

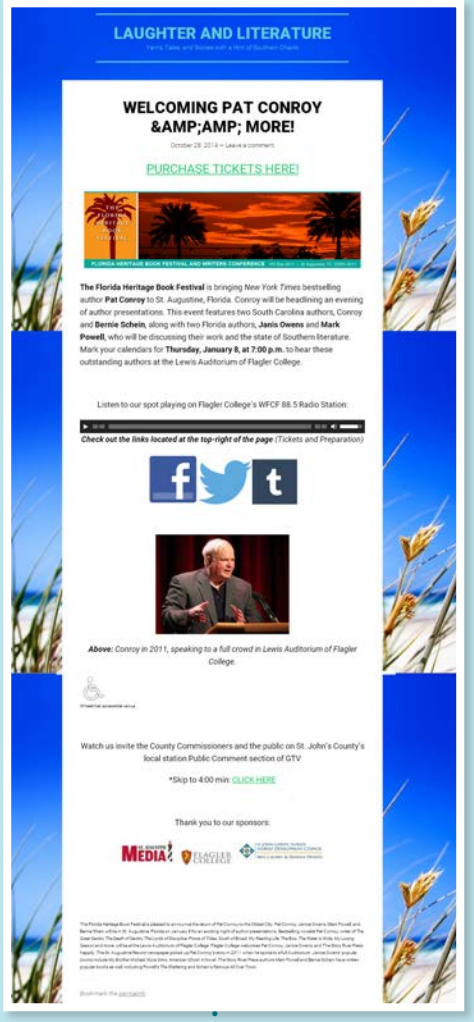
Numer przesylki	5975352707555
Produkt / serwis	DHL RETOURE
Status od czwartek, 21.05.2015 06:09:36	Przesylka zostala zaladowana na samochód do doreczenia.
Doreczono do	Przesylka zwrotna do nadawcy

Wyświetl informacje od odbiorcy
(PDF-Dokument)

Źródło: internet

JAK ROZPOZNAĆ FAŁSZERSTWO

Cechą charakterystyczną listów preparowanych przez oszustów jest niepoprawna polszczyzna i często brak polskich znaków. Wynika to wykorzystania automatycznych tłumaczy do przygotowania treści korespondencji. Część ekspertów uważa jednak, iż jest to zaplanowana strategia, zgodnie z którą najlepszym celem ataku jest osoba na tyle nieuważna, że nie potrafi ocenić nieporadności językowej, a co za tym idzie bezrefleksyjnie kliknie w podany link. Drugim znaczącym elementem jest skrzynka, z którego nadano list. I nie chodzi o oficjalną nazwę konta, bo tą niezwykle łatwo spreparować, ale o sam adres. W tym przypadku korespondencja została nadana z konta: as@escgrup.com. Domena należy do tureckiej firmy zajmującej się profesjonalnym sprzątaniem i dezynfekcją obiektów użyteczności publicznej. Również serwis, do którego przekierowuje podany w treści link, od razu zdradza oszustwo – http://patconroystaug.com/JRVti3z7GqLrd. To dla odmiany strona amerykańskiego pisarza Pata Conroya propagująca ubiegłoroczne targi książki na Florydzie.



WIRUSY I APLIKACJE

Ransomware (ang. ransom – okup) – rodzaj oprogramowania używanego w przestępczości internetowej. Działanie ransomware polega na wniknięciu do wnętrza atakowanego komputera i zaszyfrowaniu danych należących do użytkownika. Potem program umieszcza w komputerze notatkę. Przestępca pisze w niej, co musi zrobić właściciel cennych plików, aby je odzyskać. Zwykle internetowy bandyta domaga się przelania pieniędzy na konto w banku elektronicznym i obiecuje, że w zamian wyśle klucz oraz instrukcje, jak odszyfrować dane.
Źródło: pl.wikipedia.org

Cryptolocker jest niebezpiecznym programem ransomware, który blokuje personalne dane użytkownika, jego pliki, właściwie cały dostęp do maszyny, pokazując tylko użytkownikowi monit proszący o zapłacenie 300 dolarów haraczu za odblokowanie. Cryptolocker używa metody zwanej *asymetric encryption*. Oznacza to, że jeżeli chcesz odzyskać dostęp do swoich plików, powinieneś znać dwa klucze bezpieczeństwa. Podczas gdy większość programów ransomware może być usunięta za pomocą konkretnych zachować i posunięć użytkownika, tak w przypadku tego zagrożenia ciężko znaleźć drogę, aby sobie z nim poradzić tak łatwo, jak z innymi programami ransomware. Wygląda na to, że jedynym skutecznym rozwiązaniem tego problemu jest zdobycie drugiego klucza aktywacyjnego, który jest znany tylko cyberprzestępcom. W nawiązaniu do komunikatów jakie serwuje nam program, mamy tylko określony czas na zakupienie licencji, po jego upłynięciu możemy się z plikami pożegnać – zostaną usunięte.
Źródło: usunwirusa.pl

Infostealer.Banker.C – aplikacja monitoruje i rejestruje istotne informacje na temat użytkownika. Może również zablokować dane przechowywane na dysku twardym. Jest w stanie monitorować również urządzenia peryferyjne – mysz, mikrofon i kamerę internetową. Ruchy myszą, głos i zrzut obrazu z kamery mogą być przechowywane i przekazywane autorowi programu. Przestępca może w ten sposób pozyskać nazwy użytkownika, hasła, numery kart kredytowych, kont bankowych, dane rozliczeniowe i inne istotne informacje przydatne np. do kradzieży tożsamości. Aplikacja Infostealer.Banker.C może działać w tle i nie jest widoczna w menedżerze zadań systemu Windows. Aplikacja umieszcza własne kopie w wielu miejscach systemu, by odtworzyć się nawet po całkowitym usunięciu.
Źródło: www.paretologic.com