KOMENDA STOŁECZNA POLICJI

http://www.policja.waw.pl/pl/stoleczna-policja/wydzialy-ksp/wydzial-do-walki-z-cybe/31385,Wydzial-do-walki-z-Cyberprzestepczoscia.html
2021-10-23, 00:59

WYDZIAŁ DO WALKI Z CYBERPRZESTĘPCZOŚCIĄ

Data publikacji 02.10.2014

Naczelnik: mł. insp. Rafał Zatara

Zastępca Naczelnika: kom. Mariusz Mikołajczyk

fax: +48 47 723-31-38

Globalna sieć komputerowa - internet - stał się nieodłączną częścią naszego codziennego życia. Wykorzystywany jest w pracy, do nauki, wymiany informacji lub jako forma relaksu, czy zabawy. Niestety, z internetu korzystają również osoby, które wykorzystują go do popełniania przestępstw. Za pośrednictwem internetu, tak jak i w świecie rzeczywistym, popełniana jest cała gama różnego rodzaju przestępstw, jednak użytkownicy nie zawsze zdają sobie z tego sprawę, jak łatwo można stać się ofiarą cyberprzestępczości.

Ofiary cyberprzestępczości to najczęściej ofiary oszustw. Oszustwa internetowe stanowią przeważającą grupę przestępstw, która w bardzo szybkim tempie się rozwija i ewoluuje w coraz bardziej złożone formy. Poniżej opisane są niektóre rodzaje oszustw internetowych, metody działania sprawców oraz sposoby postępowania umożliwiające uniknięcia oszustwa i pozostania jego ofiarą.

ATAKI HAKERSKIE:

W wyniku ataków hakerskich przejmowane są np.: skrzynki e-mail dużych firm. Sprawcy analizują ich zawartość a następnie podszywając się pod prawowitych posiadaczy preparują nową wiadomość, w której informują kontrahentów o nowym rachunku bankowym, na który należy przesłać środki pieniężne z tytułu wzajemnych zobowiązań.

ZŁOŚLIWE OPROGRAMOWANIE:

Ataki na klientów korzystających z bankowości internetowej z wykorzystaniem np.: trojana Banatrix, polega na przeszukiwaniu przez trojan pamięci procesów przeglądarek internetowych: Chrome, Internet Explorer, Firefox oraz Opera w celu znalezienia ciągu liczb, który odpowiada numerowi rachunku bankowego, a następnie zamianie go na inny numer rachunku podstawiony przez przestępców.

BOTNET:

Grupa komputerów zainfekowanych specjalną odmianą wirusa pozostającego w ukryciu przed użytkownikiem i pozwalającego jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami “zombie” w ramach botnetu. W ramach ww. działań hakerskich dochodzi do blokowania serwisów poprzez ataki DDoS w celu uzyskania środków za przywrócenie ich funkcjonowania, zbieranie danych z przejętych komputerów i handel nimi, oszustwa i sabotaże, handel sieciami botnet.

ATAKI DDoS

Przestępcy wysyłają e–mail’a z informacją o wykryciu luki bezpieczeństwa w systemie pozwalającym na przeprowadzenie ataku DDoS. W związku z powyższym żądają zapłaty kwoty w BitCoin w ciągu 24 – 48 godz na podany w wiadomości numer portfela. W przypadku niespełnienia żądania grożą przeprowadzeniem ataku DDoS, a kwota „okupu” wzrośnie dziesięciokrotnie. W przesłanej korespondencji wskazane jest nie tylko portfel kryptowaluty, ale

również instrukcja jak zakupić BitCoin'y, a także w przypadku napotkania problemów link do czatu suportu.

KRADZIEŻ TOŻSAMOŚCI I PRANIE PIENIĘDZY

Do tego typu przestępstw dochodzi często poprzez przesłanie do użytkowników ofert atrakcyjnej pracy. Sprawcy zazwyczaj oferują wysokie wynagrodzenia lub proponują pracę nie wymagającą od przyszłych „pracowników" dużego wysiłku. Oferty pracy przychodzą na adresy mailowe w postaci spamu lub ogłoszeń, itp. Ofiara wysyła swoje CV, kopię dokumentów tożsamości, numer swojego konta bankowego i telefon kontaktowy. Zdarzają się nawet przypadki gdzie oszust wymaga od aplikantów założenia konta bankowego na swoje dane osobowe, a następnie wysłanie otrzymanej karty bankomatowej wraz z kodem PIN. Jeżeli użytkownik spełni wymagania, oszust ma wszystko co potrzebne aby posłużyć się tożsamością ofiary do popełniania innych przestępstw. Po wyłudzeniu tych informacji oszust może dalej wykorzystywać nieświadomość użytkownika.

W przypadku fałszywych ofert pracy, zadaniem ofiary jest zazwyczaj przesyłanie pieniędzy, wpływających na konto, do wskazanych przez oszustów osób czy banków. Przy czym przesyłanie pieniędzy odbywa się za pośrednictwem systemu płatności uniemożliwiającego identyfikację odbiorcy. Ofiara jest przekonana, że pieniądze pochodzą z legalnie działających firm, przesyła pieniądze w żądane miejsce za co pobiera prowizję. Ofiary nie zdają sobie sprawy, że uczestniczą w procesie tzw. „prania pieniędzy", pochodzących
z przestępstwa.

Fałszywe oferty pracy wykorzystywane są również do wyłudzania pieniędzy. Odbywa się to w podobny sposób. Oszust wysyła bardzo korzystną ofertę pracy za granicą. Ofiara odpowiada na ofertę, bardzo łatwo przechodzi rekrutację, a następnie ma zgłosić się do pracy. Oszust zapewnia, że wszystko jest już załatwione, prosi jedynie o wpłacenie niewielkiej kwoty np. na zakup biletu lotniczego, wykupienia wizy, pozwolenia na pracę czy opłacenia wynajętego mieszkania. Przestępstwo takie jest formą „oszustwa nigeryjskiego".

FAŁSZYWE OFERTY KUPNA I SPRZEDAŻY

Oszustwa dokonywane za pośrednictwem ofert kupna/sprzedaży są jedną z najstarszych metod wyłudzania pieniędzy. Najczęściej oszuści zamieszczają bardzo atrakcyjną finansowo ofertę kupna np. samochodu lub motocykla na portalu aukcyjnym. Ofiara kontaktuje się z oszustem w celu dokonania zakupu, a oszust chce otrzymać pieniądze jak najszybciej. Odbiór osobisty nie jest możliwy, gdyż oszust bardzo często przebywa właśnie za granicą i zależy mu na szybkiej sprzedaży samochodu. W celu uwiarygodnienia swojej oferty, oszuści proponują dokonanie transakcji poprzez zaufaną firmę pośredniczącą tzw. „Escrow Service", która ma gwarantować dostawę samochodu do klienta. Przy czym firma „Escrow Service" nie istnieje, jest stworzona przez oszusta. Ofiara wysyła pieniądze i na tym kontakt się urywa.

Drugą wersją tego oszustwa (choć dużo rzadszą) jest zamiar dokonania przez oszusta zakupu np. samochodu, bądź innego towaru jaki potencjalna ofiara oferuje do sprzedaży przez portal ogłoszeniowy lub aukcyjny. Schemat jest bardzo podobny. Oszust prosi o przesłanie towaru za granicę i proponuje zabezpieczenie transakcji poprzez Escrow Service – firmę pośredniczącą, gwaranta bezpiecznej transakcji. Ofiara dostaje maile od fałszywego Escrow Service, informujące że wpłata została dokonana i można wysyłać towar. Oczywiście pieniądze nigdy nie docierają do ofiary. Czasem pokrzywdzeni otrzymują wiadomości e-mail z darmowych skrzynek mailowych, imitujących znane instytucje bankowe.

OSZUSTWO NIGERYJSKIE

Oszustwo nigeryjskie (z ang. 419 Fraud, West African Fraud) - oszustwo na zaliczkę jest znane od XVI wieku, wówczas znane było pod nazwą Listu Hiszpańskiego Więźnia, a do jego popełnienia wykorzystywano pisanie i wysyłanie listów. Obecnie oszuści wykorzystują w tym celu pocztę elektroniczną. Rozsyłają wiadomości, w których piszą, że znaleźli się w bardzo trudnej sytuacji (pomysłowość jest zadziwiająca, potrafią podawać się za byłych ministrów, prawników czy nawet naszych dalekich krewnych) i proszą o pomoc w podjęciu dużej sumy pieniędzy, czy też spadku. Ofiara jest zapewniana, że otrzyma dużą część przedmiotowej kwoty w zamian za wpłacenie kwoty na np. opłaty skarbowe czy prawników prowadzących sprawę spadkową. Jest to jedna z wielu form tego oszustwa.

OSZUSTWO Z WYKORZYSTANIEM SMS

Proste oszustwo polegające na wyłudzeniu pieniędzy od osób, które za skorzystanie z usług dostępnych na różnego rodzaju stronach internetowych płacą wysyłając wiadomość tekstową SMS. Internauci otrzymują wiadomość e-mail zachęcającą np. do wykonania testu na inteligencję i sprawdzenia swojego IQ. Aby otrzymać rozwiązanie testu należy

wysłać płatną wiadomość SMS, której cena nie jest jasno sprecyzowana np. wymaga się od użytkownika aby zachował ściśle określony, kilkuetapowy sposób wysłania wiadomości.

W efekcie rachunek za tę usługę zaskakuje niemile. Kolejny przykład to wysyłanie e-kartek. Cena za wysłanie takiej kartki nie jest wysoka, wynosi kilkadziesiąt groszy. Za wysłanie płaci się SMS-em, który w rzeczywistości kosztuje użytkownika nie kilkadziesiąt groszy ale kilkadziesiąt złotych. Powodem tego jest zapis w regulaminie, według którego użytkownik płaci za sto takich kartek, o czym nie miał pojęcia.

SZANTAŻ RANSOMWARE

Wcześniej przestępcy za pomocą ransomware'u sugerowali, że za blokadą komputera stoją organy ścigania. Teraz idą o krok dalej: ich ransomware szyfruje wszystkie dane osobiste, jakie może znaleźć. Ofiary wirusa nie mogą więcej korzystać z własnych dysków i ważnych dokumentów. W kolejnych latach ten problem się zaostrzy, ponieważ tworzenie i zamawianie tego typu szkodników jest coraz łatwiejsze. Producenci ransomware'u są już dobrze zorganizowani, niektórzy oferują nawet działające linie wsparcia technicznego: pracownicy wprawdzie nie pomagają ofierze pozbyć się szkodnika, ale chętnie wyjaśniają, jak zapłacić okup.