Cyberwojna – phishing DNS w polskich instytucjach publicznych

9 listopada 2019

Poniższy artykuł jest syntezą części szerszego raportu opracowanego dla Ministerstwa Cyfryzacji oraz Fundacji Stratpoints. Link do raportu na samym końcu.

Najprościej mówiąc phishing to sposób oszustwa, którego metoda zaliczana jest do inżynierii społecznej, a polega na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji lub w celu wprowadzenia nieprawdziwych lub prawdziwych informacji w obieg tych instytucji. Najczęściej spotykanym zastosowaniem jest korespondencja e-mail od autora podszywającego się pod określoną instytucję lub organizację celem wyciągnięcia danych osobowych lub płatności elektronicznych.

Zazwyczaj odbywa się to poprzez otwarcie odnośnika do fałszywej strony, która podszywa się pod inny podmiot. Na stronie imitującej właściwy podmiot znajduje się okienko do logowania tak jak we właściwym serwisie. Wprowadzane dane są gromadzone i przekazywane do włamywacza, który wykorzystuje je do zalogowania do prawdziwego serwera. Inna technika polega na wysłaniu korespondencji e-mail z fałszywego serwera z prośbą o przesłanie jakiś informacji lub dokumentów. W ten sposób istnieje szansa, że ofiara ataku nie zauważy niewłaściwego adresu e-mail i automatycznie odpowie tak, jak odpowiedziałaby nadawcy właściwemu.

Zagrożenie phishingiem nie dotyczy wyłącznie użytkowników serwisów społecznościowych, klientów instytucji finansowych czy innych organizacji komercyjnych. Phishing stanowi realne wyzwanie dla bezpieczeństwa państwa, gdyż w szczególności

dotyczy fundamentalnych struktur instytucji państwowych. Zagrożenie płynie bezpośrednio z faktu braku powszechnej świadomości społecznej na temat tego czym charakteryzują się adresy właściwe wyżej wymienionych instytucji oraz jak sprawdzić wiarygodność danego serwisu. Przeciętny Kowalski nie wie jaki adres internetowy jest właściwy dla ABW, Sądu Rejonowego, Urzędu Skarbowego czy CBA. Zatem najprawdopodobniej jedną z pierwszych rzeczy jaką zrobi, to sprawdzenie w wyszukiwarce Google, czy pierwszy znaleziony adres jest taki sam jak ten, który został podany w źródle ataku. Problem zaczyna się jednak w momencie, kiedy adresy są różne, ale reprezentują wizualnie taką samą instytucję, a jednocześnie adres fałszywy podpięty jest bezpośrednio pod domenę prawdziwej instytucji.

Najprostszym sposobem imitacji serwera właściwego jest podpięcie się pod domenę wojewódzką lub utworzenie serwisu w domenie krótkiej. Możemy zatem zarejestrować np. domenę policja.com.pl która będzie imitować serwis właściwy policja.pl. Dla przeciętnego użytkownika w większości wypadków policja.com.pl będzie adresem podejrzanym, gdyż Policja nie jest przecież instytucją komercyjną. Natomiast w przypadku adresu Policja.Wroclaw.pl jego czujność zostanie znacznie uśpiona, gdyż Wroclaw.pl jest przecież oficjalnym portalem internetowym Wrocławia. Nie wiadomo zatem, dlaczego nie zostały zarezerwowane i zablokowane dla stron trzecich subdomeny z nazwami najważniejszych i najbardziej charakterystycznych instytucji. Nie dziwi zatem fakt, że zostały one błyskawicznie przejęte nie tylko przez komercyjnych odbiorców, ale również przez nieznane podmioty poza granicami Rzeczypospolitej Polski. Co więcej adres Policja.Wroclaw.pl może natychmiast przekierować zapytanie http na adres serwisu właściwego, natomiast pocztę transportowaną SMTP pozostawiać na serwerze atakującym.

Najbardziej narażeni są zwykli ludzie, użytkownicy Internetu, którzy nie mają powszechnej wiedzy na temat potencjalnych

zagrożeń. Ta grupa jest najliczniejsza i w największym stopniu narażona na masowe manipulacje oraz potencjalne ataki. Większość ataków pozostaje niezidentyfikowana przez ofiary, a potencjalne pytania stawiane są dopiero w przypadku zgłoszenia na policję, gdy mamy do czynienia ze stratą materialną znaczącego rozmiaru. Nie wiadomo jednak jak wiele operacji przeprowadzono oraz jaka ilość pozyskanych informacji została uśpiona na czas potencjalnego, masowego ataku. Jeżeli wydaje Ci się czytelniku, że taki scenariusz jest mało prawdopodobny, to uświadom sobie fakt, iż często czytasz dokument pobrany z internetu, którego pochodzenia tak naprawdę nie znasz, w formacie umożliwiającym wykonanie instrukcji na Twoim komputerze już w momencie, gdy pierwszy raz kliknąłeś na niego myszką, a sama liczba potencjalnych ataków np. poprzez format dokumentu .pdf liczy wiele, wiele stron. Skoro Ty właśnie w tej chwili mogłeś paść ofiarą takiego ataku, to znaczy że na Twoim miejscu właśnie mógł być ktokolwiek inny. Na szczęście tym razem nie musisz się niczego obawiać, ale potraktuj to jako osobistą przestrogę i nowe doświadczenie.

Służby specjalne i służby mundurowe są wyjątkowo narażone na zagrożenia cybernetyczne ze względu na fakt wagi pozyskanej lub utraconej informacji. Oprócz wspomnianych wyżej metod podszywania się pod inne serwery (czyli de facto inne osoby i inne instytucje), manipulacje korespondencją i informacją, istnieje szereg innych technik informatycznych, które mogą zostać wykorzystane w połączeniu z socjotechniką. Należy tutaj również szczególnie podkreślić, że zagrożeni są nie tylko sami funkcjonariusze, ale również ich najbliższe osoby czyli rodzina, która powinna być objęta szczególną ochroną. Najprostszym sposobem „dotarcia” do osoby posiadającej poświadczenia bezpieczeństwa jest droga przez media społecznościowe, z których korzystają członkowie rodziny czyli np. nastoletnie dzieci lub współmałżonek. Ostatecznie najprawdopodobniej wszyscy członkowie rodziny korzystają z tej samej sieci WiFi, a jeden zainfekowany zdalnie komputer czy telefon może skutecznie rozprzestrzenić zagrożenie przez

wszelkie inne media, w tym również router WiFi. Ten z kolei przekazuje informacje do telefonu komórkowego lub laptopa, z którym ofiara ataku nie rozstaje się w swoim miejscu pracy. Warto zatem mieć świadomość, jak wiele kroków i samodyscypliny jest niezbędne w celu utrzymania odpowiedniego poziomu bezpieczeństwa.

Nie inaczej wygląda sytuacja w przypadku wymiaru sprawiedliwości, a w szczególności policji oraz pracowników sądów. Po pierwsze w obu przypadkach mamy do czynienia praktycznie z masową skalą zjawiska. Po drugie wyciek kluczowej informacji lub wprowadzenie fałszywej informacji może doprowadzić nie tylko do upadku całej sprawy procesowej, ale również narazić na odpowiedzialność karną lub fizyczne niebezpieczeństwo poszczególne osoby. Myli się ten, kto uważa, że adwokaci, kuratorzy, radcy prawni czy policjanci nie przesyłają korespondencji do prokuratorów lub sędziów drogą elektroniczną na skrzynki służbowe i odwrotnie. Niezależnie od tego jakie mamy przepisy i procedury w tym zakresie, taka sytuacja codziennie ma miejsce. Inną szczególnie narażoną grupą są posłowie, senatorowie, radni, prezydenci, czyli ogólnie politycy. Proszę wyobrazić sobie sytuację, gdy do polityka siedzącego w pewnej komisji, na kilka godzin przed posiedzeniem, przychodzi „poufna informacja” z „zaufanego źródła” o tym, że jego kolega z ławki sejmowej prowadzi negocjacje z lobbystą zainteresowany zmianą ustawy w takim lub innym zakresie. W większości przypadków taka korespondencja będzie miała znaczący wpływ na przebieg obrad, a polityk zachowa zarówno informację, jak i jej źródło dla siebie, nie badając autentyczności oraz pochodzenia takiej korespondencji. Ciekawym procesem jest już zaobserwowany fakt korzystania z telefonów komórkowych i tabletów przez posłów w trakcie głosowania. Te urządzenia korzystają z adresów internetowych nie tylko oficjalnych skrzynek poselskich, ale również skrzynek prywatnych. Niektórzy nawet wykorzystują sejmowe adresy e-mail do logowania się w grach komputerowych ustawiając w grze komputerowej takie samo hasło jak do swojego

sejmowego konta pocztowego. Przykłady można by mnożyć.

Edukacja jest podstawową metodą obrony. Niezbędnym elementem jest kształtowanie powszechnej świadomości społecznej w zakresie tego, czym są zagrożenia cybernetyczne, jakie mogą mieć skutki oraz jak im należy przeciwdziałać. Dotyczy to zarówno zwykłych użytkowników, jak również urzędników oraz innych pracowników administracji publicznej.

Absolutnie niezbędnym elementem polityki bezpieczeństwa jest stosowanie zaufanych certyfikatów. Przeciętny Jan Kowalski musi wyrobić w sobie nawyk sprawdzania autentyczności adresu internetowego zanim wyśle korespondencję lub otworzy jakiś załącznik czy link. Jednak należy pamiętać, że adresy te muszą mieć podstawowy mechanizm umożliwiający identyfikację, czyli właśnie certyfikat zaufany oraz podpis cyfrowy wiadomości. Trzecim elementem jest powszechne stosowanie kryptografii. Nie ma absolutnie żadnego usprawiedliwienia dla przesyłania informacji pomiędzy jednostkami wojskowymi czy departamentami w ministerstwie bez zastosowania kryptografii. Zakres stosowania tego mechanizmu należy znacząco poszerzyć nie tylko w kontaktach pomiędzy poszczególnymi jednostkami, ale również pomiędzy zwykłym użytkownikiem a organizacjami. Oczywiście nie da się wszystkich zobligować do stosowania kryptografii i nie o to tutaj chodzi. Jednak z całą pewnością należy wprowadzić pewne stopniowanie w zależności od skali ryzyka i proporcjonalnie do tego ryzyka, wprowadzać rozwiązania kryptograficzne. Należy również zastanowić się nad możliwością zablokowania możliwości rejestracji pewnych adresów. Nie bardzo wiadomo dlaczego umożliwiono rejestrację dowolnych subdomen w adresach regionalnych. Pewne słowa kluczowe powinny być po prostu zastrzeżone, natomiast fałszywe serwery identyfikowane i monitorowane.

Należy szczególnie podkreślić, że paraliż infrastruktury teleinformatycznej jest współcześnie kluczowym elementem wszystkich potencjalnych ataków na państwo. Niezależnie od faktu czy jest to wojna hybrydowa o małym lub dużym zasięgu,

czy też jest to element wojny konwencjonalnej. Do skutecznego przeprowadzenia takiego ataku teleinformatycznego niezbędne jest stałe prowadzenie działań rozpoznawczych i dywersyjnych. Służby Specjalne i Służby Mundurowe powinny być szczególnie świadome istniejących zagrożeń oraz podejmować wszelkie inicjatywy zmierzające do minimalizacji potencjalnego niebezpieczeństwa w tym zakresie. Obrona teleinformatyczna jest tutaj stałym komponentem składającym się na aktywne działania prewencyjne oraz nieustanne modelowanie i usprawnianie procesów eksploatacji i zabezpieczenia systemów komputerowych. Bezpieczeństwo cybernetyczne niesie ze sobą zupełnie nowe wyzwania i zagrożenia. Nie jest to ani odległa przyszłość ani tym bardziej element mniej istotny niż bezpieczeństwo energetyczne czy bezpieczeństwo publiczne. Przeciwnie, bezpieczeństwo cybernetyczne będzie się coraz bardziej wybijać na pierwszy plan jako ten komponent, który łączy się ze wszystkimi pozostałymi.

Pełna treść raportu: Stratpoints.eu
Przygotował: Jarosław Narymunt Rożyński (Prezydent.org.pl)
Źródło: WolneMedia.net