Komentarza udzielają
EKSPERCI FUNDACJI

DNS PHISHING. W POLSKICH INSTYTUCJACH PUBLICZNYCH

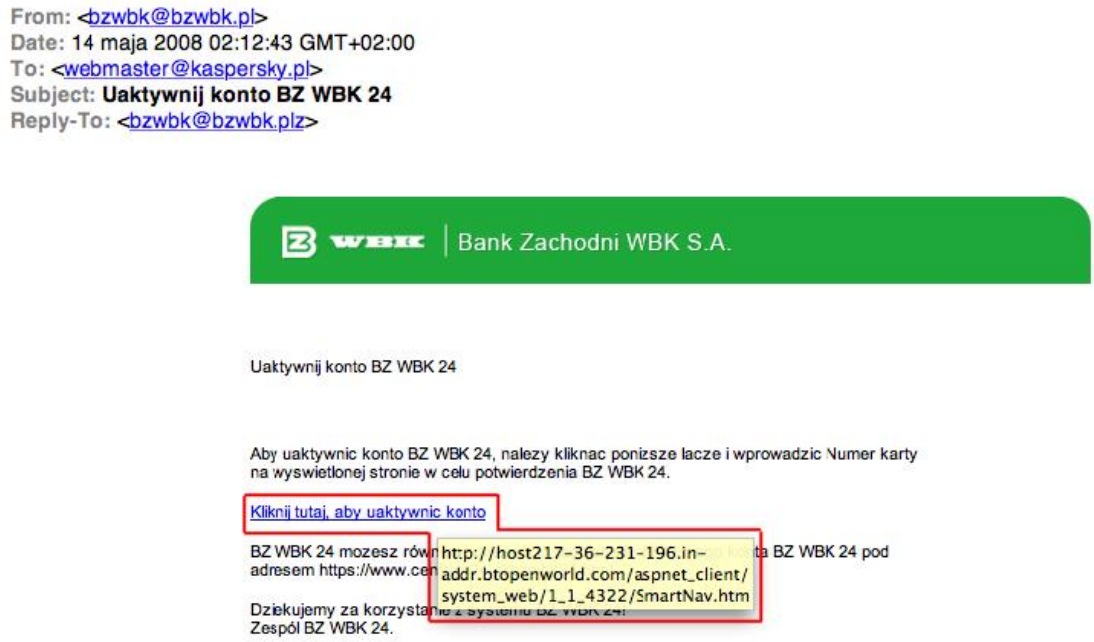
Publikacja w ramach projektu Neptune fundacji Stratpoints.

NEPTUNE
PROJEKT • BEZPIECZEŃSTWO & ROZWÓJ

1. WPROWADZENIE

Phishing

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 email 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 email z fałszywego serwera z prośbą o przesłanie jakiś informacji lub dokumentów. W ten sposób istnieje szansa, że ofiara ataku nie zauważy niewłaściwego adresu email i automatycznie odpowie tak, jak odpowiedziałaby nadawcy właściwemu.

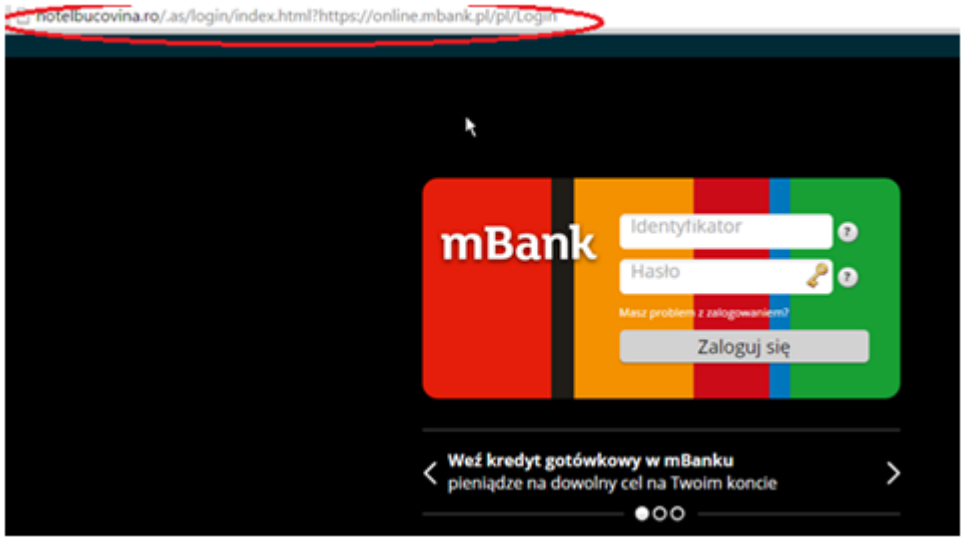


Rysunek 1 - przykład podszywania się pod Bank Zachodni WBK S.A poprzez korespondencję email z odnośnikami do fałszywej strony www

Zatruwanie DNS

Zatruwanie serwera nazw (domain name server) polega na przesłaniu przez atakującego do serwera DNS fałszywej informacji kojarzącej nazwę domeny z adresem IP. Serwer nazw zapamiętuje taką kombinację przez pewien krótki czas (do kilku godzin lub kilku minut) i zwraca swoim klientom zapamiętany adres IP. Skutkiem takiego działania jest przeniesienie odbiorcę odpytującego o daną nazwę na niewłaściwy numer IP. Niepokój użytkownika końcowego powinien szczególnie budzić fakt braku zainstalowanego certyfikatu zaufanego na stronie, którą otwiera. W szczególności dotyczy to instytucji państwowych. Na dzień dzisiejszy w Polsce niestety istnieje możliwość łatwego i legalnego podszycia się pod pewne instytucje bez stosowania ataków DNS, które zostały już praktycznie wyeliminowane poprzez rozwiązania zaimplementowane w nowych wersjach serwerów nazw. Nie mniej jednak sam problem pozostał, gdyż zmieniła się w pewnym sensie technika ataku, lecz nie zmienił

się efekt końcowy. Oprócz różnego rodzaju mechanizmów proxy, można zastosować również inne sposoby opisane poniżej.



Rysunek 2 - przykład podszywania się pod mBank poprzez przekierowanie do fałszywej strony, źródło : mBank

Pharming

Jest to najbardziej niebezpieczna dla użytkownika końcowego oraz najtrudniejsza w rozpoznaniu forma podszywania się pod inny podmiot (phishing), która polega na przekierowaniu na fałszywą stronę pomimo podania prawidłowego adresu internetowego lub podpięcie się pod prawidłowy adres internetowy w postaci subdomeny, która łączy się pośrednio lub bezpośrednio z serwerem właściwej instytucji. Teoretycznie istnieją trzy sposoby pharmingu :

1. Zatrucie globalnego serwera DNS w celu skojarzenia właściwego adresu URL z fałszywą stroną,

2. Wykorzystanie koni trojańskich do modyfikacji systemu operacyjnego w taki sposób, że będzie on przekierowywał na inne adresy niż te wskazane w odpowiedziach serwera DNS

3. Zarejestrowanie subdomeny pod domeną główną instytucji i imitacja serwisu z domeny głównej

Należy wyraźnie podkreślić, że sposób pierwszy wymaga szczególnych umiejętności technicznych i tego typu atak zdarza się stosunkowo rzadko i jest szybko nagłaśniany w mediach społecznościowych oraz w biuletynach bezpieczeństwa.

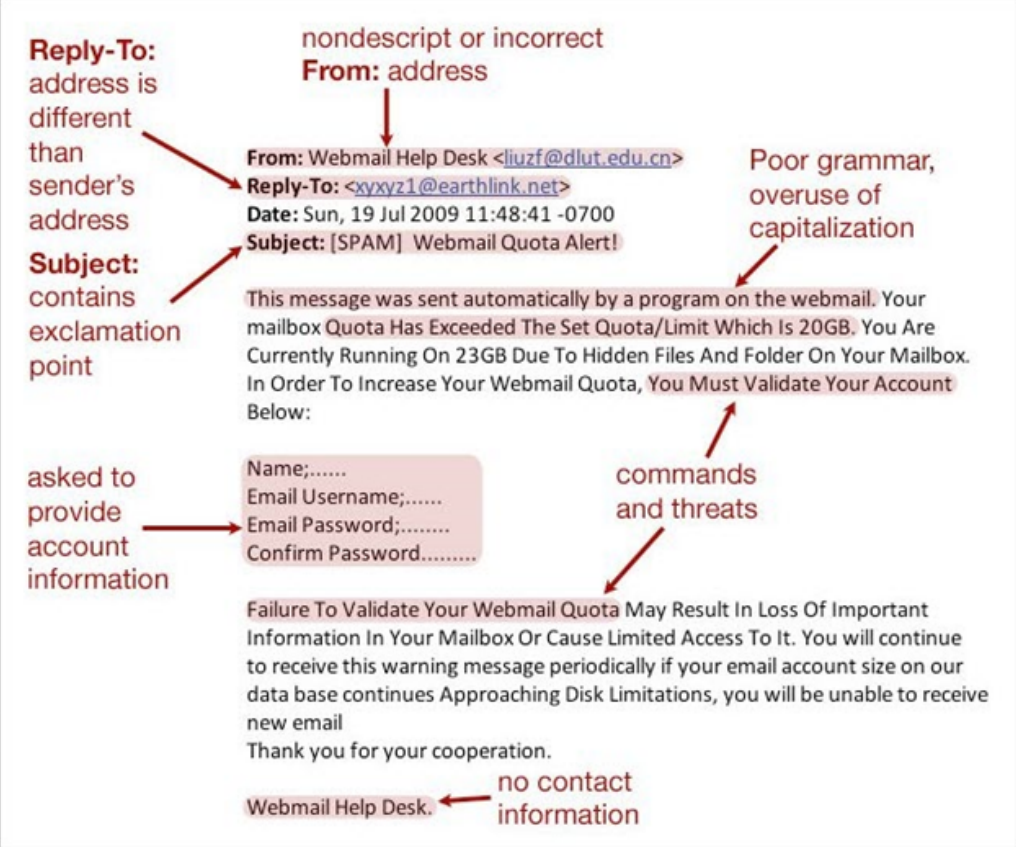
W drugim przypadku wystarczy zazwyczaj zastosować oprogramowanie antywirusowe, które zabezpiecza nas przed takimi przypadkami. Nie mniej jednak sytuacja związana z tym zagrożeniem w Polsce jest dosyć powszechna, gdyż wiele osób nie tylko nie używa oprogramowania antywirusowego, ale również regularnie pobiera pliki z serwisów pirackich (TOR, torrent, inne p2p), gdzie instalatory zawierają dodatkowe komponenty, które nie tylko modyfikują zapytania DNS, ale również mogą podpinać rejestratory klawiatury (keylogger), generatory kryptowalut i inne oprogramowanie szpiegujące. Nie jest tajemnicą, że spora część oprogramowania pirackiego w języku polskim pochodzi bezpośrednio z Federacji Rosyjskiej (np. niektóre pirackie wersje polskiej wersji Windows 7 mają podmienione kilkanaście standardowych sterowników, które zgłaszają swoją obecność serwerom w Petersburgu i odbierają instrukcje poleceń wraz z harmonogramem).

Trzeci sposób jest praktycznie transparentny, trudny do wykrycia przez stronę trzecią oraz powszechnie stosowany w przypadku polskich instytucji. Tutaj również nie jest tajemnicą, że większość przekierowań pośrednio lub bezpośrednio prowadzi do Federacji Rosyjskiej, co nie oznacza, ze za atakami stoją bezpośrednio Rosjanie. Po prostu Federacja Rosyjska jest wygodnym i łatwo dostępnym miejscem do ataku teleinformatycznego.

E-mail spoofing

Jest to technika ataku, w której dane nagłówkowe korespondencji email nadawcy zostały zmodyfikowane w taki

sposób, aby wyglądały na pochodzące z innego źródła. Najczęściej spotykanym zastosowaniem jest tutaj oczywiście rozsyłanie niezamawianej treści reklamowej (spam). Innym powszechnym zastosowaniem jest właśnie phishing, czyli rozsyłanie korespondencji podszywającej się pod organizację właściwą z linkami do fałszywych adresów www. Jednym z elementów w ramach tej techniki jest podawanie różnych adresów nadawcy i domyślnego adresu do odpowiedzi. Absolutna większość aplikacji do czytania korespondencji nie wyświetla szczegółów struktury korespondencji, a to właśnie tutaj znajdują się krytyczne informacje umożliwiające identyfikacje takiego potencjalnego ataku. Dopiero wyświetlenie pełnej struktury korespondencji wraz z nagłówkiem pokazuje jakie są różnice i zagrożenia.



Rysunek 3 - przykład struktury korespondencji wykorzystanej do e-mail spoofing, proszę zwrócić uwagę na różnicę w adresie nadawcy i adresie do odpowiedzi

DNS crossfix

DNS crossfix to nic innego jak krzyżowanie adresów nazw. Technika jest banalnie prosta i sama w sobie nie stanowi potencjalnego zagrożenia. Dopiero w połączeniu z innymi technikami stanowi istotne uzupełnienie całości. W skrócie polega ona na tym, że serwer DNS jest oddzielony od serwera właściwego, na którym skonfigurowana jest dodatkowo lub osobno inna nazwa domeny niż w serwerze nazw. Przykładowo serwer DNS będzie wskazywał, iż IP serwera podszywającego się policja.wroclaw.pl to 192.168.1.1 natomiast sam serwer będzie przy poczcie przychodzącej i wychodzącej identyfikował się jako wroclaw.policja.gov.pl, gdyż będzie to wynikało z jego lokalnej konfiguracji. Ponieważ serwer nazw a serwer właściwy to osobne maszyny, nie będzie tutaj istniał konflikt. Co więcej serwer nazw nie widzi konfiguracji serwera podszywającego się, a poczta przekazywana jest bezpośrednio do numeru IP a nie do adresu domeny. Jest to szczególnie istotne w przypadku konfiguracji serwera „pod łowienie poczty", gdzie zależy atakującemu na przyjmowanie wszystkich informacji, które ominęły serwer właściwy. Dodatkowym rozwiązaniem jest tutaj również ustawienie reguł dla poczty przychodzącej ACCEPT_ALL, co spowoduje, że poczta będzie trafiała do naszych skrzynek nie tylko w przypadku pomyłki w nazwie domeny, ale nawet w przypadku pomyłki w adresie skrzynki. Zwykłe mapowanie skrzynek pocztowych w konfiguracji serwera pocztowego zwiększa znacząco prawdopodobieństwo „złapania" większej ilości korespondencji przychodzącej do podszywającego się serwera. Przykładowa konfiguracja serwera Sendmail będzie wyglądać podobnie do następującej :

```
define(`SMART_HOST',`local:some_user')dnl
define(`MAIL_HUB',`local:some__user')dnl
```

dnl optional part to list local users/mailboxes excluded from
the redirect
dnl in /etc/mail/direct-users file (one user per line)
LOCAL_CONFIG
FL/etc/mail/direct-users
divert(0)

Dodatkowo w /etc/hosts znajdą się w przykładowej konfiguracji następujące wpisy :

127.0.0.1 localhost
192.168.1.1 policja.wroclaw.pl
192.168.1.1 wroclaw.policja.gov.pl

W przypadku uruchomienia lokalnie obu komend z podszywającego się serwera otrzymamy taką samą odpowiedź z adresu 192.168.1.1:
ping policja.wroclaw.pl
ping wroclaw.policja.gov.pl

Natomiast z zewnątrz ping wskaże oczywiście na dwa różne adresy, gdyż odwoła się do innych, właściwych serwerów nazw (DNS).

2. ZAGROŻENIA DLA PAŃSTWA

Cele ataku

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.

Metody ataku

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. Przykładowy skrypt umieszczony w pliku index.php na stronie głównej podszywającego się serwera wystarczy by wprowadzić użytkownika w błąd, kiedy pomyśli on, iż adres fałszywy, a rzeczywisty to w istocie ten sam serwer, a w istocie są to zupełnie różne serwery:

```
<?php
header('Location: http://wroclaw.policja.gov.pl/pl/');
?>
```

Umieszczenie powyższego na dowolnym serwerze http z obsługą php spowoduje przeskoczenie przeglądarki na adres http://dolnoslaska.policja.gov.pl/pl/

Zatem w tym konkretnym przypadku zapytania http zostają przeniesione, natomiast poczta pozostaje na serwerze w subdomenie. Jednakże, aby całość miała większy sens, należy w subdomenie utworzyć konta pocztowe odpowiadające kontom rzeczywistym w domenie macierzystej oraz wprowadzić fałszywe adresy do obiegu. Nie potrzeba do tego wyszukanych narzędzi, gdyż wystarczy dowolna

dystrybucja Linuxa z obsługą sendmail. W przypadku Slackware będzie to wyglądało następująco :

```
cd /usr/share/sendmail/cf/cf
sh Build sendmail-slackware.mc
cp sendmail-slackware.cf /etc/mail/sendmail.cf
cp submit.cf /etc/mail/
chmod +x /etc/rc.d/rc.sendmail
/etc/rc.d/rc.sendmail start
```

Kolejnym krokiem jest utworzenie skrzynek podszywających się pod adres rzeczywisty, co jest również elementem trywialnym (adduser). Wystarczy bowiem dokładnie obejrzeć macierzystą stronę internetową, by takie adresy odnaleźć. Dodatkowo można pokusić się o przeszukanie portali społecznościowych i odnaleźć pracowników danej instytucji, a następnie na fałszywym koncie z ładnym zdjęciem podszywającym się np. pod atrakcyjną modelkę poprosić o podanie służbowego emaila. Istnieje prawdopodobieństwo, że wiele osób poda takie adresy w przekonaniu, że nic im nie grozi, gdyż są to przecież ich oficjalne adresy służbowe.

Co więcej, na samej stronie internetowej znajdują się często adresy w innych domenach niż domena strony internetowej, co tym bardziej wprowadza w zamieszanie użytkowników.

Przykład (różne przedrostki w adresie domen) :

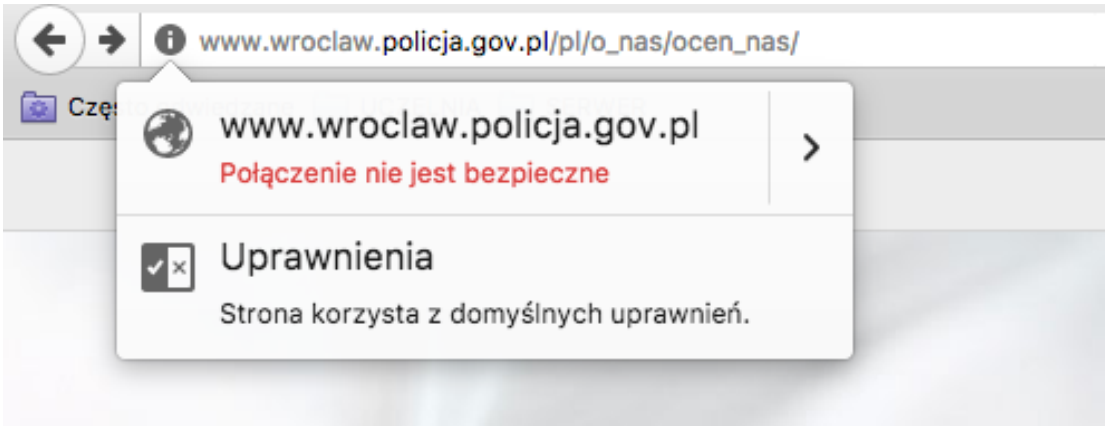
Adres URL **:**
http://www.**wroclaw**.policja.gov.pl/pl/o_nas/kierownictwo/
Adres email na powyższej stronie :
kontakt@**wroclaw.wr.**policja.gov.pl

Oczywiście, gdy do przeglądarki WWW wprowadzimy adres wroclaw.wr.policja.gov.pl taki jak w adresie email – nie wyświetli się żadna strona. Zatem użytkownik może pomyśleć, że adres jest niewłaściwy i skorzysta z następnego w kolejce. Co więcej, sam klient pocztowy (aplikacja) może dokonać takiego odpytania w trakcie sortowania książki adresowej i umieścić właściwy adres mailowy na końcu listy podpowiedzi.

Nie wzbudzi zatem powszechnego podejrzenia fakt istnienia dodatkowej skrzynki o nazwie kontakt@policja.wroclaw.pl która będzie w rzeczywistości adresem prowadzącym do podszywającego się serwera podpiętego bezpośrednio pod Dolnośląski Urząd Wojewódzki.

Mając zatem utworzoną już skrzynkę kontakt@policja.wroclaw.pl (adres na fałszywym serwerze), można przystąpić do cross-pharmingu, czyli np. odpytania urzędu skarbowego o dane osobowe podejrzanego lub rozesłać masowo do różnych instytucji życzenia świąteczne z zajączkiem w załączniku. W ten sposób adres nie tylko służy do „rozsiewania" złośliwego oprogramowania, ale również do „pozycjonowania się" w książkach adresowych innych instytucji.

W celu jeszcze większego zamaskowania atakującego stosuje się technikę e-mail spoofing oraz DNS crossfix. Subtelna różnica w nagłówku email jest jeszcze bardziej trudna do odnalezienia nawet przez oprogramowanie antywirusowe, zwłaszcza w sytuacji, gdy na serwerze właściwym nie ma zainstalowanego zaufanego certyfikatu. Należy dodać, że strony praktycznie wszystkich instytucji w Polsce są niezabezpieczone zaufanymi certyfikatami tożsamości. Wystarczy kliknąć na ikonkę obok adresu instytucji, by przekonać się o tym na własne oczy.



Rysunek 4 - weryfikacja bezpiecznego połączenia i certyfikatu domeny

Szczególnym przypadkiem beztroski jest tutaj również Ministerstwo Obrony Narodowej, które praktycznie wszystkie najważniejsze adresy korespondencyjne umieszcza na stronie WWW pod adresem : http://www.mon.gov.pl /kontakt

Nie trudno również wyobrazić sobie jakie skutki i zamieszanie może zostać wprowadzone przed ćwiczeniami wojskowymi, gdy nagle jednostki wzajemnie zaczną przesyłać między sobą fałszywe informacje lub część informacji zostanie przekazana do niewłaściwych serwerów. W pierwszym przypadku sam fakt pojawienia się danej informacji będzie skutkował co najmniej koniecznością zweryfikowania źródła i autentyczności. W drugim przypadku, znacznie trudniejszym do wykrycia, oprócz weryfikacji źródła ataku niezbędne będzie oszacowanie strat, oszacowanie ryzyka oraz podjęcie działań zapobiegawczych. Niestety jak wskazują powyższe przykłady, nie jest to problem do rozwiązania na poziomie pojedynczej jednostki wojskowej lub nawet na poziomie jednego województwa, organizacji czy ministerstwa.

Ważną informacją jest również fakt, że cała procedura imitacji może być uruchomiona i zlikwidowana w ciągu dosłownie kilkunastu minut. Całą operację można zatem przeprowadzić z laptopa w

kawiarence internetowej. Nie trudno zatem wyobrazić sobie sytuację, gdy hacker uruchamia serwis podszywający się pod policję lub inną instytucję, przesyła zapytania lub dokumenty do prokuratury lub innego organu z fałszywych adresów email, po czym po otrzymaniu odpowiedzi likwiduje cały łańcuch zależności prowadzący do niego. Ponieważ korzysta z publicznego połączenia WiFi, nie istnieje w praktyce łatwy sposób namierzenia jego tożsamości. Co więcej, może on tego dokonać w sposób w pełni transparentny nawet bez korzystania z subdomeny regionalnej, jeżeli jego celem jest jedynie wprowadzenie informacji do obiegu, a nie pozyskanie informacji z serwisu głównego.

Szczególnie narażone podmioty

1. ABW

Agencja Bezpieczeństwa Wewnętrznego ma swój serwis główny w domenie abw.gov.pl. Jednak większość użytkowników w pierwszej kolejności wprowadza adres abw.pl lub podobny, który szczęśliwie prowadzi na stronę firmową podmiotu zarejestrowanego w Polsce. Jednak już zupełnie inaczej wygląda sprawa subdomeny „abw" w przypadku domen wojewódzkich, gdzie część serwerów znajduje się na terenie Ukrainy i Federacji Rosyjskiej, a niektóre z nich zarejestrowane są w Holandii czy na Cyprze.

Oczywiście mało prawdopodobna jest sytuacja, by ktoś odwoływał się do serwisu abw.wolomin.pl czy podobne, jednak subdomena abw.warszawa.pl jest już znacznie bardziej narażona na tego typu manipulacje.

2. Centralne Biuro Antykorupcyjne

Podobnie jak powyżej, wygląda sytuacja w przypadku CBA, gdzie serwisem głównym jest cba.gov.pl, a najczęściej wpisywaną nazwą jest jednak cba.pl.

W przypadku subdomen również mamy do czynienia z ciekawą sytuacją. Niektóre adresy zarejestrowane w postaci subdomen w domenach regionalnych prowadzą albo do Holandii, albo do Krakowa, albo do innych lokalizacji poza granicami Polski. Pozostałe są w większości wolne do rejestracji. Nie wiadomo jednak, czy niektóre strony są tymczasowe oraz jaki ruch odbywa się na pozostałych portach i usługach poza http.

3. Ministerstwo Obrony Narodowej

W przypadku Ministerstwa Obrony Narodowej mamy do czynienia z dużą ilością domen oficjalnych. Należą do nich nie tylko subdomeny .gov.pl, ale również .mil.pl. Większość odbiorców nie jest jednak w stanie zorientować się, która nazwa jest właściwa, czy np. http://11ldkpanc.wp.mil.pl czy http://11ldkpanc.zagan.pl w sytuacji gdy obie strony będą wyświetlać to samo. Nie istnieje również centralny, rządowy rejestr, właściwych adresów stron internetowych jednostek wojskowych. Łatwo można zatem manipulować nie tylko korespondencją, ale również przepływającymi informacjami.

Zupełnie niezrozumiała jest również praktyka prowadzenia blogów jednostek wojskowych, czy też tworzenia stron struktur wojskowych na portalach społecznościowych. Zdaje się, że na dzień dzisiejszy Polska jest chyba jedynym państwem NATO, gdzie kadra najwyższego stopnia prowadzi blogi i kłóci się przez Twitter i Facebook w zakresie koncepcji właściwej strategii obronnej. Te

konta bardzo często powiązane są z ich telefonami, które łączą się z routerami znajdującymi się w jednostkach. Samo przełączenie się pomiędzy sieciami nie jest zabezpieczeniem (albo korzystam z jednej albo z drugiej), a telefony wniesione na teren jednostki wojskowej lub ministerstwa łączą się z innymi telefonami i sukcesywnie rozprowadzają mechanizmy ataku. Do zaatakowania innego urządzenia w ogóle nie musi być używana sieć WiFi / TCP, wystarczy Bluetooth i odpowiednia odległość jednego urządzenia od drugiego. Ostatni atak masowy przy wykorzystaniu takiego rozwiązania miał miejsce 7 listopada i zdarza się kilka razy w miesiącu :

https://blog.pointas.com.pl/lokibot-nowy-trojan-bankowy-uzytkownicy-stracili-juz-15-mln-dolarow/

Nie jest również tajemnicą fakt, że część jednostek wojskowych korzysta z oprogramowania, na które licencja już dawno wygasła. Dotyczy to zarówno oprogramowania desktop jak również sterowników innych urządzeń. Taka sytuacja jest niedopuszczalna, niestety nagminna.

4. Urzędy Skarbowe

Urzędy skarbowe zazwyczaj posiadają krótkie adresy składające się z przedrostka „us" oraz nazwy lokalizacji. Większość tych adresów, które podpięte są pod wojewódzkie lub miejskie domeny regionalne, prowadzi donikąd. Przykładowo us.bialystok.pl prowadzi na serwer w Katowicach, a wyniki wyszukiwania frazy „urząd skarbowy Białystok" prowadzą na szereg serwerów stron trzecich. Bardzo podobnie wygląda sytuacja w przypadku pozostałych kilkuset domen regionalnych. Nie istnieje jeden mechanizm umożliwiający jednoznaczne odróżnianie stron instytucji podległych Ministerstwu Finansów. Istnieje zatem szerokie pole do manipulacji w tym zakresie.

5. Zakład Ubezpieczeń Społecznych

Nie inaczej wygląda sytuacja w przypadku ZUS, gdzie również mamy szereg domen zarejestrowanych na serwerach nie należących do tej instytucji. Np. adres zus.bialystok.pl prowadzi do serwisu „Zdrowie, Uroda i Sport", podczas gdy jest to najczęściej wpisywany adres przy wyszukiwaniu Zakładu Ubezpieczeń Społecznych w tym województwie. Po prostu ten adres jest aktualnie lepiej wypozycjonowany w wyszukiwarkach.

Niestety nie każdy ma świadomość, że istnieje tylko jeden serwis główny. Bez problemu można zatem zarejestrować serwis w subdomenie regionalnej i wprowadzić innych użytkowników w błąd.

6. Policja

Bardzo poważnie wygląda sytuacja w przypadku Policji. Część adresów podpiętych do domen regionalnych przekierowuje pod właściwe adresy serwerów policyjnych. Niestety pozostała część prowadzi albo donikąd albo pod fałszywe adresy. Przykładowo po wpisaniu adresu policja.katowice.pl zostaniemy przeniesieni pod właściwy adres http://www.katowice.slaska.policja.gov.pl/ lecz w przypadku policja.radom.pl znajdziemy się w serwisie aftermarket, a już serwer inny serwer policja w domenie regionalnej, prowadzi bezpośrednio do Niemiec (Bayern/Gunzenhausen). Istnieje także wiele subdomen regionalnych, a w szczególności wojewódzkich, które mogą zostać przejęte przez strony trzecie.

Co więcej, wiele komisariatów prowadzi aktywnie profile w mediach społecznościowych i zdarzały się już przypadki, gdy na oficjalnych kontach mylono nazwy innych komend. Wynika to

bezpośrednio z faktu, ze nie jest uporządkowany system domen dla tych konkretnie jednostek administracji publicznej.

7. Urzędy Wojewódzkie i Urzędy Miejskie

W przypadku wyszukiwania urzędu miejskiego lub wojewódzkiego, użytkownik w większości przypadków wpisuje nazwę urzędu oraz nazwę miejscowości. Nie budzi zatem podejrzeń użytkownika korespondencja otrzymana z adresu uw.[województwo].pl

Drugim poważnym zagrożeniem są wolne subdomeny eup/esp oraz bip, które analogicznie stosowane były dla serwisów Elektronicznej Skrzynki Podawczej jak również Biuletynu Informacji Publicznej. W większości przypadków istnieje możliwość zarejestrowania subdomen w domenach oficjalnych instytucji regionalnych zarówno na poziomie województwa jak również poszczególnych miast.

8. Sądy i prokuratura

Podobnie jak dla urzędów wojewódzkich i urzędów miejskich wygląda sytuacja w przypadku sądów i prokuratur. Schemat domen to zwykle [miasto].sr.gov.pl dla sądów rejonowych i [miasto].so.gov.pl dla sądów okręgowych. Jednak większość internautów wprowadzi do wyszukiwarki np. sad.gdansk.pl lub sad.warszawa.pl oczekując, że pod tym adresem pojawi się strona sądu. Wynika to bezpośrednio z tego, że adresy instytucji właściwych są nieintuicyjne. Adresy można by tutaj mnożyć, gdyż istnieje ponad 200 domen regionalnych.

(Wszystkie domeny i serwisy docelowe sprawdzone przez NASK oraz serwis http://whoisrequest.com/ , stan na 7 listopad 2017r. Serwis

IP-LOCATION podaje że np. abw.bydgoszcz.pl znajduje się we Francji, a inne adresy na Ukrainie lub na terenie Federacji Rosyjskiej).

Szczególnie narażone osoby

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 czytasz dokument, 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 poprzez format dokumentu .pdf liczy wiele, wiele stron. (http://goo.gl/CGoPXu) 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 email do logowania się w grach komputerowych ustawiając w grze komputerowej takie samo hasło jak do swojego sejmowego konta pocztowego. Przykłady można by mnożyć.

3. METODY OBRONY

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.

4. WNIOSKI

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.

| PUBLIKACJE

www.stratpoints.eu