Prezentujemy Wam siódmy numer naszego S.M.S.-owego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte”.

Spis treści

Wstęp

Przygotowaliśmy dla Was siódmy numer naszego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte” analizujący zagrożenia 2020 roku. Znów macie możliwość zajrzenia do naszej infrastruktury i przekonania się z jakimi podatnościami mierzymy się codziennie. Zapraszamy również do zapoznania się z pierwszym numerem biuletynu, gdzie szczegółowo opisujemy powody dla, których postanowiliśmy tworzyć takie materiały.

Standardowo biuletyn składa się z 3 głównych części – ogólnej analizy statystycznej incydentów w naszej infrastrukturze, analizy przypadku jednego z wybranych przez nas zagrożeń oraz podsumowania całego zebranego przez nas materiału. Na końcu dodaliśmy również sekcję „Poprzednie numery”, co pozwoli Ci łatwo znaleźć wcześniejsze wydania biuletynu.

Numer kwietniowy również powstawał we współpracy z Fudo Security. Dzięki temu, że umożliwili nam testowanie swojego rozwiązania Fudo PAM, dalej mogliśmy monitorować nasze sesje oraz sprawdzać co uda nam się złowić na naszym firewall’u. Aby dowiedzieć się, więcej o samym Fudo Security oraz sprawdzić nad czym pracują wpadnijcie na ich profile w social mediach – LinkedIn, Twitter, Facebook. Koniecznie dajcie znać, że przysłało Was S.M.S.!

Chcielibyśmy również zachęcić naszych kolegów z branży do przyłączenia się do naszej inicjatywy i współpracy przy tworzeniu kolejnych wydań biuletynu. Jeśli masz pomysł jak wykorzystać Twój potencjał, pomysł lub produkt w materiale serdecznie zapraszamy do kontaktu mailowego w celu ustalenia szczegółów: blog@s-m-s.pl.

Mamy nadzieję, że zapoznanie się z materiałem sprawi Ci tyle satysfakcji ile nam sprawiło jego przygotowanie. Zapraszamy również do dyskusji na jego temat we wszystkich dostępnych kanałach – sekcja komentarzy na naszym blogu, nasze profile w social mediach (Facebook oraz Twitter) czy też pod adresem mailowym: blog@s-m-s.pl. Każda opinia na ten temat jest dla nas ważna i pomoże nam ulepszyć kolejne wydania biuletynu.

Miłej lektury!

Ogólna analiza statystyczna incydentów

W celu określenia skali i częstotliwości występowania zdarzeń w infrastrukturze najlepszym będzie przeanalizowanie dostępnych danych statystycznych. Dzięki takiemu zabiegowi będziemy mogli w sposób kompleksowy przedstawić kwestie cyberbezpieczeństwa naszej infrastruktury. Na potrzeby przygotowania tej części materiału wykorzystaliśmy technologię umożliwiającą nam stałe monitorowanie ruchu do naszych serwerów. Pozwoliło nam to wyszczególnić zdarzenia, które zostały przedstawione poniżej. Podobnie jak w poprzednich wydaniach badaniu poddane zostały dane zebrane z własnych narzędzi służących do administrowania ruchem do serwerów.

Przeanalizowaliśmy dane za okres od 01.04.2020 do 30.04.2020. Do analizy statystycznej użyte zostały takie parametry jak dzienna liczba zdarzeń, najczęściej występujące incydenty, podział zagrożeń ze względu na rodzaj oraz potencjalną dotkliwość zdarzenia. W badanym okresie odnotowaliśmy znaczący spadek prób ingerencji w nasze systemy. Udało nam się wyodrębnić 28.864 zdarzeń w kwietniu. Średnia liczba zagrożeń w tym miesiącu wyniosła 962 zdarzeń dziennie. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w kwietniu

W kwietniu ponownie liczba prób kompromitacji naszych serwerów była bardzo zmienna. Często liczba zdarzeń jednego dnia przekraczała 1.000. Tym razem wybraliśmy 2 dni – 12.04.2020 0raz 20.04.2020. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – odpowiednio 6.117 oraz 2.766. Poniżej prezentujemy tabele, w których przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	Liczba zagrożeń
MS-RDP Brute-force Attempt	5900
UNIX Portmapper Remote Infomation Retrieving Attempt	117
ZmEu Scanner Detection	27
HTTP Directory Traversal Vulnerability	20
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	26
HTTP Non RFC-Compliant Response Found	9
MySQL Authentication Brute-force Attempt	8
FTP: login Brute-force attempt	5
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	3
HTTP OPTIONS Method	1
OpenSSL TLS Heartbeat Information Disclosure Vulnerability - Reverse Heartbleed	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 12.04.2020 r.

Rodzaj zagrożenia	Liczba zagrożeń
MySQL Authentication Brute-force Attempt	2300
UNIX Portmapper Remote Infomation Retrieving Attempt	129
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	175
SSH User Authentication Brute-force Attempt	45
ZmEu Scanner Detection	42
DNS RRSIG Query Type Packet	31
HTTP Directory Traversal Vulnerability	19
HTTP Non RFC-Compliant Response Found	16
FTP: login Brute-force attempt	4
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	2
OpenSSL TLS Heartbeat Information Disclosure Vulnerability - Reverse Heartbleed	1
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	1
DistCC Daemon Command Execution	1

Tab. nr 2 Typy zdarzeń oraz ich liczba
w dn. 20.04.2020 r.

Przedstawiamy Wam też nasz Top 19, czyli listę najbardziej popularnych zagrożeń w kwietniu. Są to najczęściej wykorzystywane typy zagrożeń, poprzez użycie których atakujący próbowali skompromitować naszą infrastrukturę. Poniżej tabela zagrożeń wraz z liczbą zdarzeń.

Rodzaj zagrożenia	Liczba zagrożeń
MySQL Authentication Brute-force Attempt	9500
MS-RDP Brute-force Attempt	7200
UNIX Portmapper Remote Infomation Retrieving Attempt	3200
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	2413
HTTP SQL Injection Attempt	1581
ZmEu Scanner Detection	1400
FTP: login Brute-force attempt	1400
HTTP Directory Traversal Vulnerability	1100
DNS RRSIG Query Type Packet	437
HTTP Non RFC-Compliant Response Found	273
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	138
HTTP Unauthorized Brute-force Attack	118
SSH User Authentication Brute-force Attempt	114
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	60
HTTP OPTIONS Method	36
HTTP Cross Site Scripting Vulnerability	19
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	17
MailEnable IMAP Server Long Tag anomaly	12
DNS Zone Transfer AXFR Attempt	11

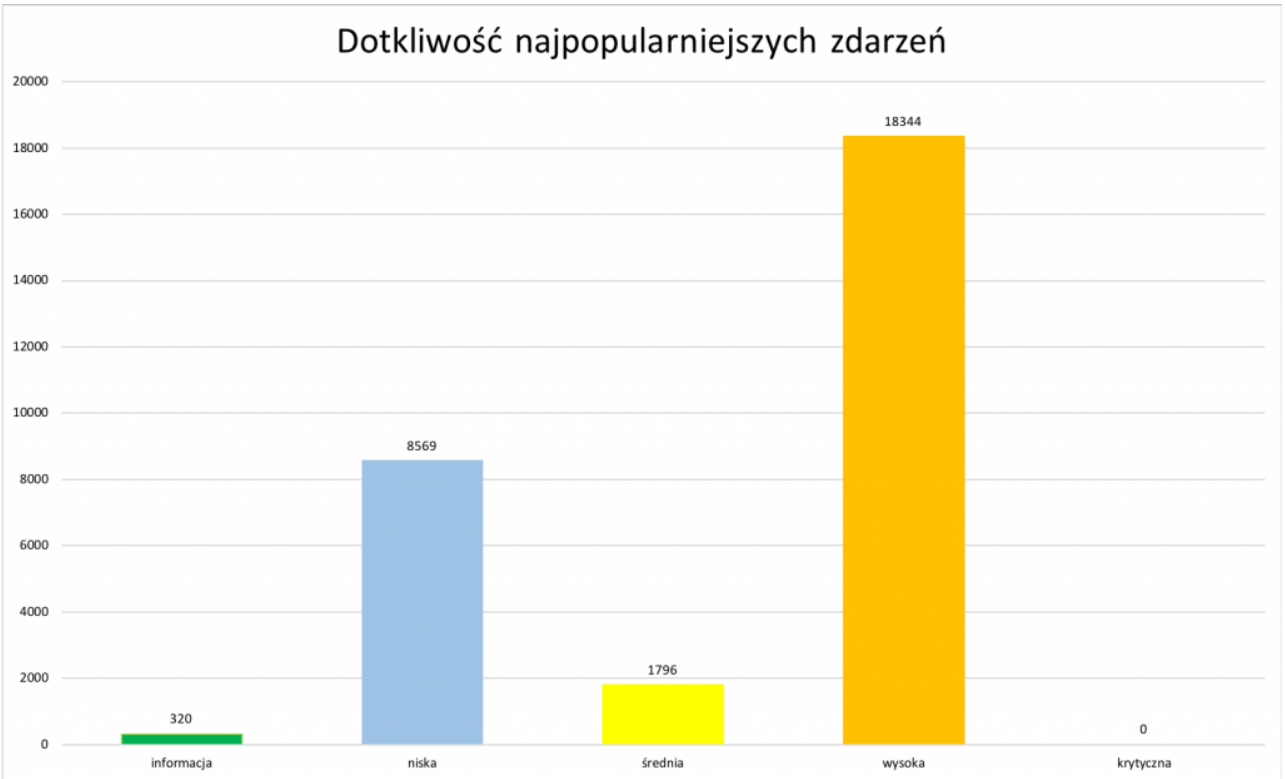
Tab. nr 3 Typy zdarzeń oraz ich
liczba w kwietniu

Jak można zauważyć oprócz bardziej popularnych zdarzeń, które regularnie umieszczamy na tej liście od początku publikacji biuletynu, ponownie pojawia się nowe zagrożenie, które stało się szczególnie istotne w dobie pandemii – a mianowicie „MS-RDP Brute-force Attempt". Próba ingerencji w systemy za pomocą właśnie tej podatności jasno świadczy o tym, że atakujący zaczęli wykorzystywać obecną sytuację związaną z rozprzestrzenianiem się epidemii wirusa na świecie. Za wektor ataku w tej sytaucji obrana zostaje konieczność pracy zdalnej, co w większości przypadków wiąże się z koniecznością połączenia się z komputerem służbowym poprzez zdalny pulpit. Więcej na ten temat pisaliśmy w poprzednim numerze biuletynu, więc jeśli jeszcze go nie czytaliście to polecamy nadrobić zaległości i zapoznać się dokładnie jak zdalny pulpit może zostać wykorzystany do ataku oraz dlaczego powinniśmy zwracać większą uwagę na monitoring sesji zdalnych.

Wyżej wspominamy o pojęciu potencjalnej dotkliwości zdarzenia. Jak sama nazwa wskazuje jest to szacowany zakres szkód jakie może wyrządzić dana podatność w naszej infrastrukturze o ile dojdzie do jej pomyślnego wykorzystania. Samą dotkliwość można podzielić na 5 różnych poziomów:

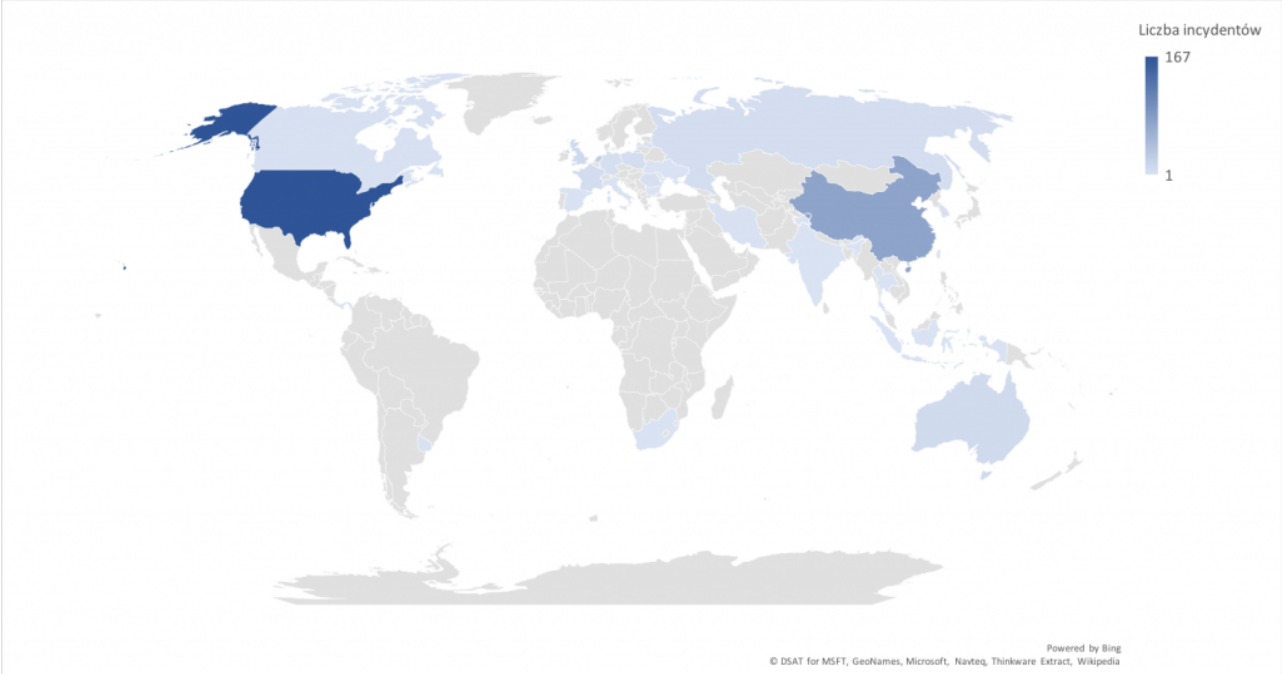
- Informacja – podejrzane zdarzenie, które nie stanowi bezpośredniego zagrożenia, ale poprzez samo jego zgłoszenie uwaga administratora może zostać zwrócona na głębsze problemy infrastruktury, które mogą zaistnieć w przyszłości.
- Niska – najniższy poziom dotkliwości wymagający ostrzeżenia. Zagrożenie ma znikomy wpływ na infrastrukturę organizacji. Zazwyczaj wymagają lokalnego bądź fizycznego dostępu do systemu i często mogą powodować problemy z prywatnością ofiary lub problemy powiązane z DoS oraz możliwy wyciek danych.
- Średnia – niewielkie zagrożenie, którego wpływ na infrastrukturę jest minimalny. Następstwem wykorzystania podatności z tej kategorii mogą być ataki typu DoS, które nie zagrażają celowi lub exploity, które od osoby atakującej wymagają przebywania w tej samej sieci LAN co ofiara. Zagrożenia poziomu średniego mogą mieć wpływ jedynie na niestandardowe konfiguracje oraz mało znane aplikacje. Zapewniają atakującemu bardzo ograniczony dostęp.
- Wysoka – zagrożenie, które potencjalnie może stać się krytycznym, jednak dzięki występowaniu czynników łagodzących nie jest możliwa jego eskalacja. Do kategorii zagrożeń poziomu wysokiego można zaliczyć zagrożenia, które są trudne do wykorzystania, nie dają podwyższonych uprawnień lub są w stanie dotknąć małej ilości ofiar.
- Krytyczna – zagrożenie poważne, które jest stanie dotknąć domyślnych instalacji szeroko rozpowszechnionego oprogramowania. Skutkuje kompromitacją serwera, a kod exploitacji jest powszechnie dostępny. Atakujący zwykle nie potrzebuje żadnych specjalnych danych uwierzytelniających ani wiedzy na temat poszczególnych ofiar, a cel nie musi być zmanipulowany w celu wykonywania jakichkolwiek specjalnych funkcji.

Na poniższym wykresie przedstawiliśmy potencjalną dotkliwość najpopularniejszych zdarzeń występujących w badanym okresie.



Wykres nr 2 Potencjalna dotkliwość najpopularniejszych zdarzeń w badanym okresie.

Podobnie jak ostatnio chcieliśmy sprawdzić z jakich krajów najczęściej pochodziły ataki. Aby to zrobić ponownie wykorzystaliśmy napisany przez nas program w bashu, który identyfikował adresy IP i przypisywał każdemu z nich kraj ich pochodzenia, a następnie je zliczał. W ten sposób otrzymaliśmy 350 unikalnych adresów IP wraz z ich krajem pochodzenia. Tym samym udało nam się zidentyfikować 28 krajów, z których próbowano skompromitować nasze usługi. Wszystkie atakujące nas państwa pokazaliśmy na poniższej mapie. Im ciemniejszy i bardziej nasycony kolor tym więcej ataków z danego miejsca odnotowaliśmy.



Mapa nr 1 Kraje próbujące atakować infrastrukturę S.M.S. w badanym okresie.

Analiza przypadku wybranych zgłoszeń

„To ciało należało kiedyś do gościa, który nie był tak dobrym stalkerem jak ja.”

Ten cytat to podobno ostatnie słowa Ivana Horna wypowiedziane tuż przed tym, jak wszedł w anomalię zwaną wirem. Zapis ten odczytano z jego PDA, który znaleziono kilkadziesiąt metrów od wiru. Z samego Ivana Horna znaleziono tylko palec.

Każdy kto grał w S.T.A.L.K.E.R.’a wie, że najgroźniejsze są anomalie. Natomiast jeśli ktoś nie grał, też powinien to wiedzieć – w końcu pisaliśmy o tym w jednym z poprzednich biuletynów. Tym razem postanowiliśmy zwrócić uwagę (co dla wielu może okazać się osobliwe i niepotrzebne) na jeden z najrzadziej pojawiających się incydentów.

Mianowicie mowa tu o „DNS Zone Transfer AXFR Attempt”. Jest to kolejna opisywana przez nas trywialna podatność, która jak mogło by się wydawać obecnie nie ma prawa bytu. Niestety, poważny problem pojawia się w momencie kiedy domyślną konfiguracją dla

serwerów DNS jest pozwolenie na transfer domeny.

Określenie transfer domeny, może mylnie sugerować, że chodzi o przeniesienie domeny. Nic bardziej mylnego. Zapytanie „axfr" jest wykorzystywane przez serwery DNS w klastrze do informowania pozostałych, jakie domeny i subdomeny mają być rozgłaszane. Zapytacie pewnie: „I co z tego?". Przecież każdy wie jaką mam domenę, a skoro nie mogą mi jej ukraść, to nie mój problem.

No właśnie Twój, administratora serwera bądź administratora danych osobowych, jeśli takowe przetwarzasz. Dla przykładu:

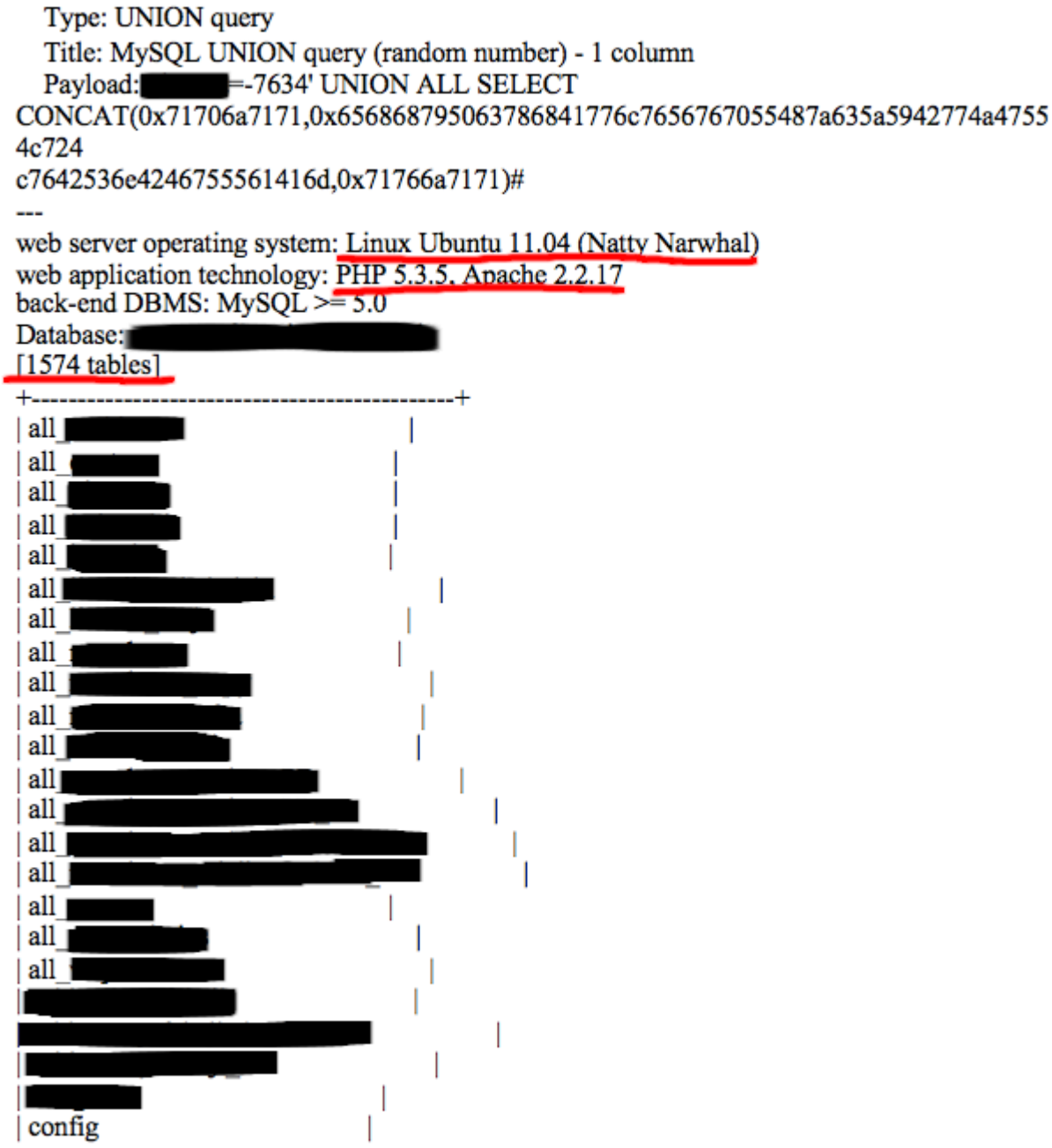
Twoja główna domena mieści się na www.domena.pl – pod tym adresem można znaleźć aktualny CMS, dobrze zabezpieczone logowanie, pewnie nawet jakieś dodatkowe zabezpieczenia. Gratulujemy. W przypadku, gdy jesteś przeciętnym posiadaczem strony www, twój wynik zapytania „axfr" wygląda następująco:

```
; <<>> DiG 9.10.3-P4-Debian <<>> axfr domena.pl @localhost
;; global options: +cmd
; Transfer failed.
root@ichibanme:~# dig axfr domena.pl @ns2.s-m-s.pl

; <<>> DiG 9.10.3-P4-Debian <<>> axfr domena.pl @ns2.s-m-s.pl
;; global options: +cmd
domena.pl.              14400   IN      SOA     ns1.domain.tld. root.domena.pl. 2020052701 7200 3600 1209600 180
domena.pl.              14400   IN      MX      10 mail.domena.pl.
domena.pl.              14400   IN      TXT     "v=spf1 a mx ip4:79.137.31.33 ~all"
domena.pl.              14400   IN      NS      ns1.domain.tld.
domena.pl.              14400   IN      NS      ns2.domain.tld.
domena.pl.              14400   IN      A       79.137.31.33
_dmarc.domena.pl.       14400   IN      TXT     "v=DMARC1; p=none"
ftp.domena.pl.          14400   IN      A       79.137.31.33
imap.domena.pl.         14400   IN      A       79.137.31.33
mail.domena.pl.         14400   IN      A       79.137.31.33
pop.domena.pl.          14400   IN      A       79.137.31.33
smtp.domena.pl.         14400   IN      A       79.137.31.33
www.domena.pl.          14400   IN      A       79.137.31.33
domena.pl.              14400   IN      SOA     ns1.domain.tld. root.domena.pl. 2020052701 7200 3600 1209600 180
;; Query time: 49 msec
;; SERVER: 194.182.77.130#53(194.182.77.130)
;; WHEN: Wed May 27 13:29:55 CEST 2020
;; XFR size: 14 records (messages 1, bytes 398)
```

Na powyższym zrzucie ekranu widzimy wylistowane wszystkie składniki domeny. Było to możliwe, ponieważ zapytanie wyszło z hosta „ichibanme", który posiada autoryzację do przesyłania takiego zapytania. Są to pozornie niegroźne dane. Niestety powyższe informacje mogą zostać wykorzystane przez potencjalnego atakującego. Jako, że ta część biuletynu jest częścią praktyczną, chcielibyśmy przedstawić scenariusz ataku z wykorzystaniem opisywanego transferu domeny, którego przebieg oparliśmy o dane z wykrytych przez nas podatności w 2017 roku.

Na stronie pewnego urzędu – ówcześnie mało zauważanego, a dziś poniekąd dyktującego Polakom jak mają żyć – zauważono błąd pozwalający na przeprowadzenie, z bardzo dużym powodzeniem, ataku typu SQL Injection. Podczas tego ataku została skompromitowana cała baza danych. Jak się okazało, jednostka ta, przechowywała wszystkie bazy danych do swoich stron www na jednym serwerze bazodanowym. Atakujący bez trudu pozyskał dane dotyczące strony www, która była wektorem ataku. Jednak jak się okazało nie posiadała ona żadnego panelu zarządzania.

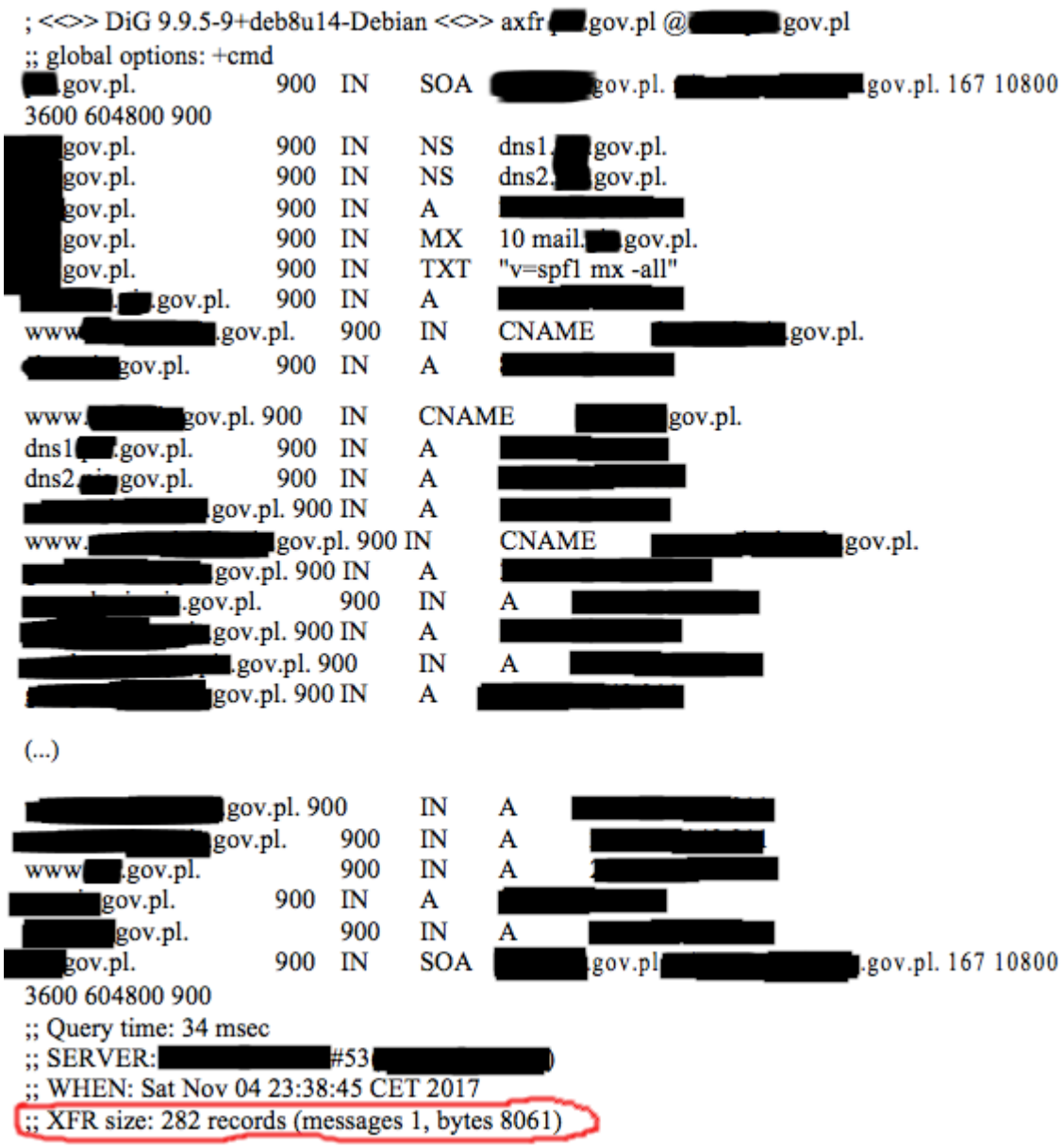


Patrząc na powyższy zrzut ekranu, warto zwrócić uwagę na kilka szczegółów:

- Dane zostały umieszczone w jednej bazie danych w taki sposób, że widzimy łącznie ponad 1500 tabel. Oznacza to, że podczas sytuacji, gdy kompromitacji ulegnie login i hasło do jednej bazy, atakujący ma dostęp do 1500 tabel z prawie 200 stron www.
- Powyższy screen powstał w październiku 2017 roku. Można zauważyć wersję systemu

operacyjnego używanego w tamtym czasie – jest to Ubuntu 11.04 (Natty Narwhal), którego end-of-life nastąpił 28 października 2012 roku, czyli 5 lat przed wykonaniem zrzutu. Nasuwa się więc pytanie: „Czy w ciągu tych 5 lat, mimo tego, że repozytoria były martwe ktokolwiek próbował robić aktualizację systemu?”.
- Wersja apache istniejącego na serwerze (2.2.17) posiada 24 potwierdzone podatności, na każdą jest dostępny exploity. Pierwsza podatność została znaleziona w 2011, a ostatnia w 2018.

W tym momencie z „pomocą” atakującemu przychodzi właśnie transfer domeny. Za jego pomocą wylistowane zostały wszystkie składniki domeny, co mówiąc wprost, pozwoliło odkryć zarówno jakie inne strony znajdują się na serwerze, a także znaleźć stronę z dostępnym panelem użytkownika, który pozwolił na dalszą kompromitację infrastruktury urzędu.



Jak widzimy na powyższym zrzucie ekranu łącznie w DNS pojawiły się 282 wpisy.
W porównaniu z 14 wpisami standardowymi widać jak dużo informacji było zawartych na serwerze.

Na szczęście ta sytuacja wydarzyła się tylko częściowo, a zanim doszło do potwierdzonej kompromitacji zgłosiliśmy znalezione podatności do instytucji. W tym miejscu musimy wspomnieć, że działania urzędu w zakresie naprawy błędów można określić jako nieudolne, ponieważ na ich poprawienie czekaliśmy ponad rok. Warto dodać, że w tym czasie

regularnie kontaktowaliśmy się, a właściwie próbowaliśmy kontaktować wszystkimi możliwymi kanałami, zarówno z pracownikami urzędu odpowiedzialnymi za bezpieczeństwo jak i z osobami odpowiedzialnymi za kontakt z mediami. Jakąkolwiek reakcję udało nam się uzyskać po upływie roku. Wtedy po kontakcie z rzecznikiem prasowym, wymogliśmy poprawki oraz naprawę błędów.

Hint:

Niestety w większości wersji serwera DNS zarówno tych na Windows jak i unixowych transfer domeny jest domyślenie dozwolony. Ułatwia to zestawianie konfiguracji, jednak po jej zakończeniu należy niezwłocznie wyłączyć transfer domeny dla hostów spoza naszej listy – uproszczając transfer domeny tylko dla serwerów DNS, które mają propagować naszą domenę.

Jako, że po poprzednie biuletyny zdobyły duży pozytywny feedback, a to o co prosiliście najczęściej to praktyczne porady jak unikać pojawiających się zagrożeń postanowiliśmy opisać jak ustawić w właściwy sposób wasze serwery.

Linux:

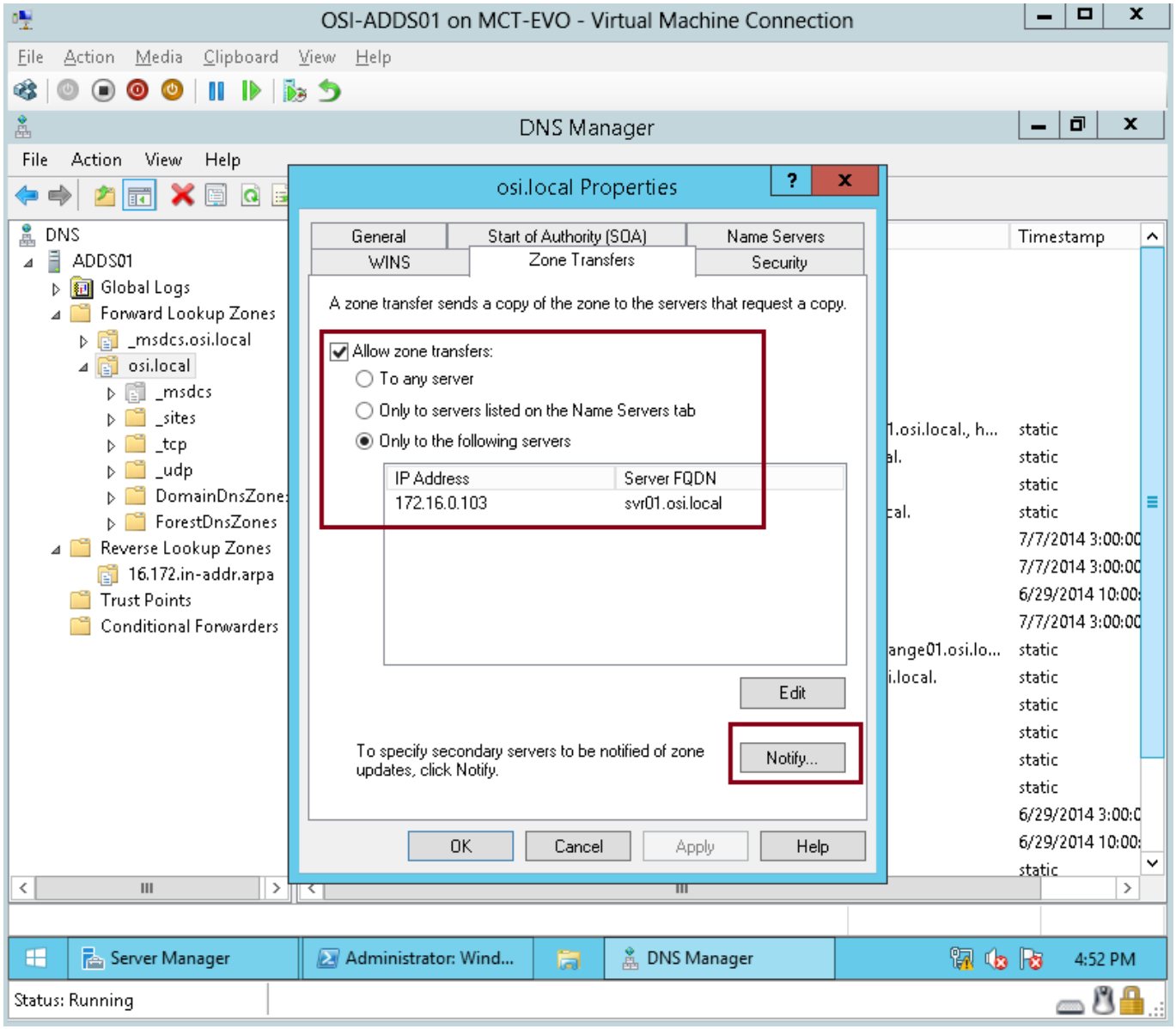
Najczęściej wybieranym serwerem DNS na unixach jest pakiet Bind, W jego przypadku w pliku /etc/bind/named.conf należy umieścić następującą linijkę:

```
allow-transfer { xxx.xxx.xxx.xxx; yyy.yyy.yyy.yyy; };
```

gdzie xxx.xxx.xxx.xxx i yyy.yyy.yyy.yyy to adresy IP zaufanych serwerów DNS, którym zezwalamy na transfer DNS.

Windows server:

W przypadku Windows Server musimy przejść do ustawień serwera i tam zmienić ustawienia dotyczące transferu domeny. Poniższy screen pochodzi z artykułu opisującego jak krok po kroku poprawnie skonfigurować strefę DNS i jej transfer. Zachęcamy Was, aby po skończonej lekturze biuletynu również zapoznać się z jego treścią.



Źródło:
https://mizitechinfo.wordpress.com/2014/07/07/step-by-step-configure-dns-zone-transfer-in-windows-server-2012-r2/

Podsumowanie

Po raz kolejny zwracamy waszą uwagę na prosty błąd w konfiguracji i wykorzystanie trywialnej podatności. Mimo, że wydają się być banalne, to ich skutki zdecydowanie mogły doprowadzić do poważnego wycieku danych, a co za tym idzie utraty wiarygodności oraz kompromitacji prezentowanej instytucji.

Niektórzy mogą nam zarzucić, że się powtarzamy jednak my na pierwszym celu stawiamy sobie edukację i podnoszenie świadomości. Dlatego z tego miejsca ponownie apelujemy do Was – pamiętajcie, że błędów nie popełnia tylko ten, który nic nie robi. Pamiętajcie o regularnym sprawdzaniu waszych konfiguracji celem wychwycenia błędów i usunięcia potencjalnych wektorów ataku.

Poprzednie numery

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 1 10/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 2 11/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 3 12/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 4 01/20

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 5 02/20

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 6 03/20

Post powstał we współpracy z Fudo Security. Nie jest to materiał sponsorowany, a wszystkie opinie zawarte w biuletynie należą do S.M.S. i są jedynie naszymi spostrzeżeniami. Serdecznie dziękujemy kolegom i koleżankom z Fudo Security za umożliwienie nam testowania rozwiązania Fudo PAM.