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

Spis treści

Wstęp

Przygotowaliśmy dla Was ósmy 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 01.05.2020 do 31.05.2020. 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 39.956 zdarzeń w maju. Średnia liczba zagrożeń w tym miesiącu wyniosła 1.289 zdarzeń dziennie. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w maju

W maju ponownie liczba prób kompromitacji naszych serwerów była bardzo zmienna. Często

liczba zdarzeń jednego dnia przekraczała 1.000. Dlatego tym razem wybraliśmy jeden dzień, podczas którego liczba zdarzeń była zdecydowanie wyższa czyli 30.05.2020. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – 4.694. Poniżej prezentujemy tabele, w których przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	Liczba zdarzeń
OpenSSH AES-GCM Auth Remote Code Execution Vulnerabillity	2902
MySQL Authentication Brute-force Attempt	678
HTTP SQL Injection Attempt	565
FTP: login Bruce-force attempt	341
HTTP Directory traversal vunerabillity	102
Unix Portmapper Remote Information Retrieving Attempt	38
DNS RRSIG QUERY TYPE PACKET	27
HTTP Unatuhorized Brute-force Attack	21
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerabillity	8
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	7
WordPress Cuckootap Theme Arbitrary File Download Vulnerabillity	4
HTTP Unatuhorized Brute-force Attack	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 30.05.2020 r.

Przedstawiamy Wam też nasz Top 20, czyli listę najbardziej popularnych zagrożeń w maju. Są to najczęściej wykorzystywane typy zagrożeń, poprzez użycie których atakujący próbowali skompromitować naszą infrastrukturę. Poniżej tabela zagrożeń wraz z liczbą zdarzeń.

Rodzaj zagrożenia	Liczba zdarzeń
OpenSSH AES-GCM Auth Remote Code Execution Vulnerabillity	18633
MySQL Authentication Brute-force Attempt	10956
Unix Portmapper Remote Information Retrieving Attempt	2724
FTP: login Bruce-force attempt	2274
SSH User Authentication Brute-force Attempt	2072
HTTP SQL Injection Attempt	1763
HTTP Directory traversal vunerabillity	743
DNS RRSIG QUERY TYPE PACKET	319
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerabillity	169
ZmEu Scanner Detection	145
WordPress Cuckootap Theme Arbitrary File Download Vulnerabillity	65
HTTP OPTIONS Method	58
DNS Zone Transfer AXFR Attempt	13
WordPress MailPoet Newsletters Unauthenticated File Upload Vulnerabillity	9
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	7
DNS Zone Transfer AXFR Response	2
Bash Remote Code Execution Vulnerability	1
DNS Answer Big TXT Record Response Anomaly	1
HTTP Unatuhorized Brute-force Attack	1
SSL Double Client Hello Cipher Suite Length Mismatch	1

Tab. nr 3 Typy zdarzeń oraz ich liczba w maju

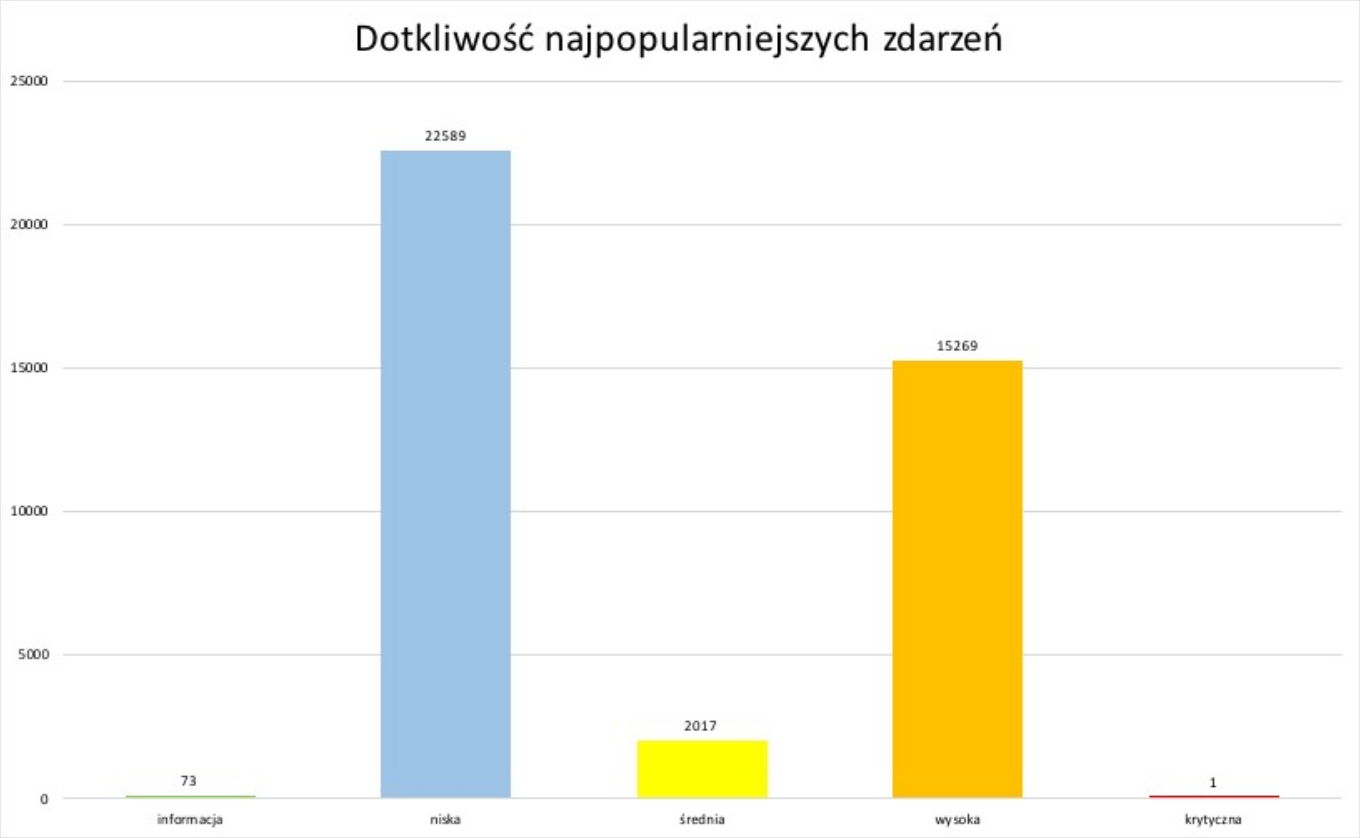
Wyżej wspominamy o pojęciu potencjalnej dotkliwości zdarzenia. Jak sama nazwa wskazuje jest to szacowany zakres szkód jakie może wyrządzić dana podatność w naszej infrastrukturze o ile dojdzie do jej pomyślnego wykorzystania. Samą dotkliwość można podzielić na 5 różnych poziomów:

- 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.

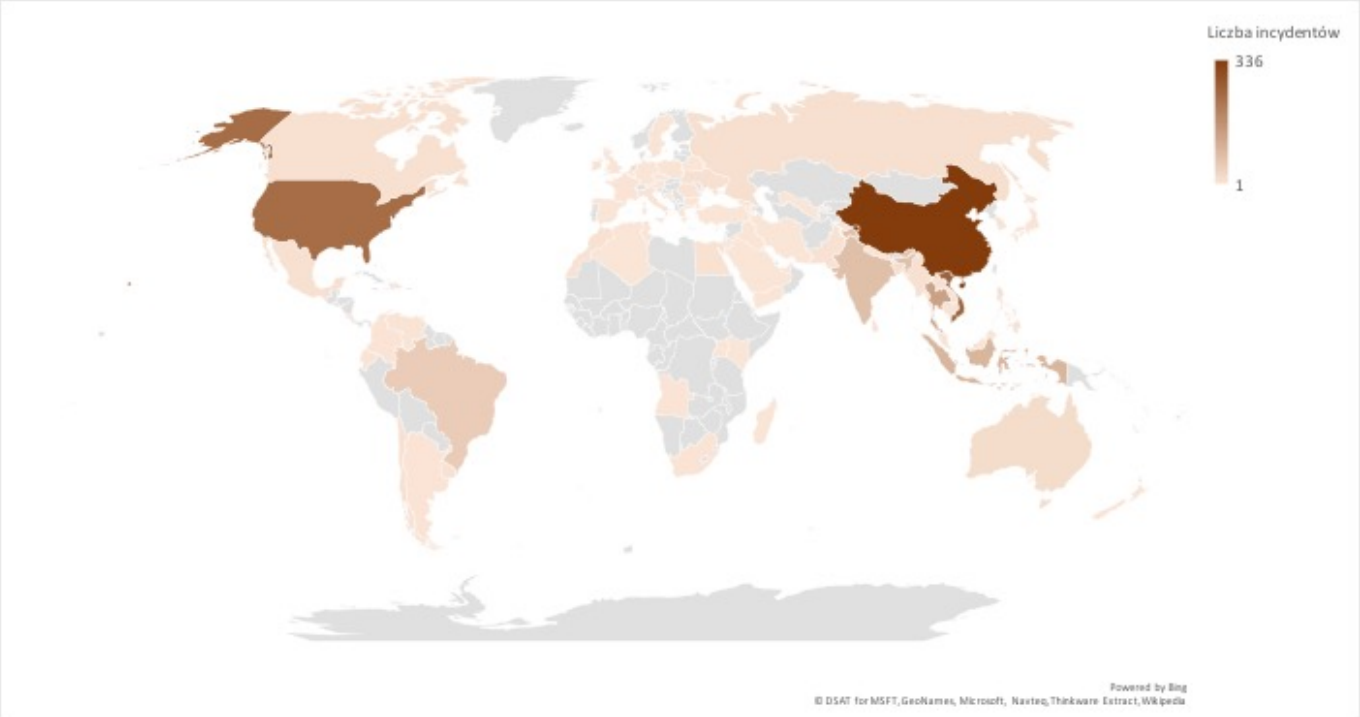
- Średnia – niewielkie zagrożenie, którego wpływ na infrastrukturę jest minimalny. Następstwem wykorzystania podatności z tej kategorii mogą być ataki typu DoS, które nie zagrażają celowi lub exploity, które od osoby atakującej wymagają przebywania w tej samej sieci LAN co ofiara. Zagrożenia poziomu 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 1.492 unikalnych adresów IP wraz z ich krajem pochodzenia. Tym samym udało nam się zidentyfikować 79 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

Problem wycieków danych jest wałkowany od początku „internetów”. Zawsze w magiczny sposób „coś” wychodziło na zewnątrz – od numeru telefonu, przez loginy i hasła po dane dostępowe do rachunków bankowych. Prawdę mówiąc, zazwyczaj za tego typu działanie odpowiedzialny jest bezmyślny użytkownik, który w poważaniu ma jakiekolwiek zalecenia czy wskazówki, w jaki sposób chronić siebie i swoją tożsamość. Zdarza się jednak, że lukę, przez którą nieuprawnieni użytkownicy mogą wykraść dane spowodowali sami twórcy gotowego rozwiązania np. webowego.

Żeby była jasność. Poniższy tekst nie ma na celu nikogo oczernić, a sam temat wycieku danych za sprawą użytkownika na pewno poruszymy w przyszłości. Dzisiaj jednak chcielibyśmy się skupić na błędzie w rozszerzeniu Heartbeat dla protokołów szyfrujących (TLS oraz DTLS), który wyszedł na świat w 2011 roku. Podatność ta w naszych systemach monitorowania ruchu na serwerach nosi nazwę „OpenSSL TLS Malformed Heartbeat Request Found – Heartbleed”.

Zanim zaczniemy, może bardzo krótko o samym Heartbeat. Jest to rozwiązanie zaproponowane w celu testowania, kontrolowania i podtrzymywania łączy komunikacyjnych, bez konieczności nawiązywania połączenia za każdym razem. Nazwa związana jest z tym, że rozszerzenie wymusza przesył pewnej ilości danych od klienta do serwera i odwrotnie – jak bicie serca.

Na czym właściwie polega cała dziura w systemie? Heartbleed (trzeba przyznać, że świetnie odniesienie nazwy buga do nazwy rozszerzenia) pozwala na odczyt pamięci systemów, które zostały zabezpieczone przez wadliwą wersję biblioteki OpenSSL. Autorzy biblioteki na swojej stronie stwierdzają, że może dojść do wycieku nawet 64kb pamięci. W tym może zawierać się wszystko – hasła, identyfikatory sesji, a nawet klucze prywatne certyfikatów SSL. Generalnie to atakujący może zrobić co chce – wykraść po prostu dane, podszyć się pod daną usługę lub po prostu podsłuchać komunikację pomiędzy serwerem a klientem. Warto wspomnieć, że odbieranie danych może następować w trybie ciągłym, tzn. atakujący

może przyjmować fragmenty danych i ponawiać atak, aż do uzyskania interesujących go informacji.

No dobrze, a czy można się jakoś ochronić przed tym?

Ano można. Przede wszystkim podatność Heartbleed dotyczy wersji OpenSSL od 1.0.1 do 1.0.2-beta włącznie. Obecnie będziemy wkraczać w wersję 3.0.0. Technologia trochę się zmieniła.

Drugim sposobem jest po prostu zablokowanie tego „problemu” w systemie typu firewall (takich, jak np. PaloAlto Networks). W dużym uproszczeniu wystarczy włączyć filtrowanie rekordów SSL z typem „heartbeat” i problem w zasadzie się rozwiązuje.

Na koniec ciekawostka – by przyśpieszyć pracę nad łatką naprawiającą ten błąd, utworzono specjalne logo (wrzucone powyżej) oraz stronę internetową o tematyce Heartbleed. Warto wejść nawet z czystej ciekawości i dowiedzieć się kilku rzeczy na ten temat https://heartbleed.com/.

Podsumowanie

Kolejny raz przedstawiliśmy Wam analizę przypadku w naszym stylu. Ustaliliśmy problem, w tym wypadku wycieki danych, które z pozoru mają jedną, główną przyczynę – nieuwaga, nieświadomość oraz błąd użytkownika końcowego. Zagłębiając się dokładniej w temat znaleźliśmy z pozoru prostą podatność, którą do swojego rozwiązania wprowadza sam jego twórca. Samo zabezpieczenie się przed nią nie powinno stanowić większego problemu dla administratora. Jednak skutki jakie niesie za sobą w przypadku nieprawidłowej konfiguracji sieci i systemów są o wiele bardziej destrukcyjne oraz mogą stać się kompromitacją dla całej firmy. Dlatego kolejny raz podkreślamy jak istotne jest sprawdzanie własnych konfiguracji, aktualizacja ustawień oraz ciągły monitoring usług.

Poprzednie numery

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.