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

Spis treści

Wstęp

Przygotowaliśmy dla Was czwarty 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.

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 miesiącach, badaniu poddane zostały dane zebrane z własnych narzędzi służących do administrowania ruchem do serwerów. Przeanalizowaliśmy dane za okres od 01.01.2020 do 31.01.2020. Do analizy statystycznej użyte zostały takie parametry jak dzienna liczba zdarzeń, najczęściej występujące incydenty, podział zagrożeń ze względu na rodzaj oraz potencjalną dotkliwość zdarzenia. Nowy rok okazał się być dla nas niemałym zaskoczeniem pod względem potencjalnych incydentów. W badanym okresie odnotowaliśmy 11.175 prób ingerencji w nasze systemy, co oznacza, że liczba ta wzrosła ponad dwukrotnie w porównaniu do poprzedniego miesiąca. Średnia liczba zagrożeń w tym miesiącu wyniosła w przybliżeniu 360 dziennie. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w styczniu

W styczniu ponownie liczba prób kompromitacji naszych serwerów utrzymywała się średnio na stałym poziomie. Nasze zainteresowanie przykuły dwa dni – 09.01.2020 oraz 30.01.2020. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – w sumie odpowiednio 3.630 0raz 2.607 zagrożeń. Poniżej prezentujemy tabele, w których przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	Liczba
HTTP SQL Injection Attempt	3588
UNIX Portmapper Remote Infomation Retrieving Attempt	30
HTTP Non RFC-Compliant Response Found	8
DNS Zone Transfer AXFR Attempt	2
MailEnable IMAP Server Long Tag anomaly	1
DNS Zone Transfer AXFR Response	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 09.01.2020 r.

Rodzaj zagrożenia	Liczba
HTTP SQL Injection Attempt	2536
UNIX Portmapper Remote Infomation Retrieving Attempt	51
HTTP OPTIONS Method	11
HTTP Non RFC-Compliant Response Found	6
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	1
JavaScript Obfuscation Detected	1
MailEnable IMAP Server Long Tag anomaly	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 30.01.2020 r.

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

Rodzaj zagrożenia	Liczba
HTTP SQL Injection Attempt	6728
FTP: login Brute-force attempt	1800
UNIX Portmapper Remote Infomation Retrieving Attempt	1100
HTTP Non RFC-Compliant Response Found	339
ZmEu Scanner Detection	247
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	168
HTTP Directory Traversal Vulnerability	101
HTTP OPTIONS Method	67
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	31
Web Vulnerability Assessment	24
MailEnable IMAP Server Long Tag anomaly	22
Bash Remote Code Execution Vulnerability	19
Invalid HTTP Version Found	14
DNS Zone Transfer AXFR Attempt	11
DNS Zone Transfer AXFR Response	10
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	4
JavaScript Obfuscation Detected	3

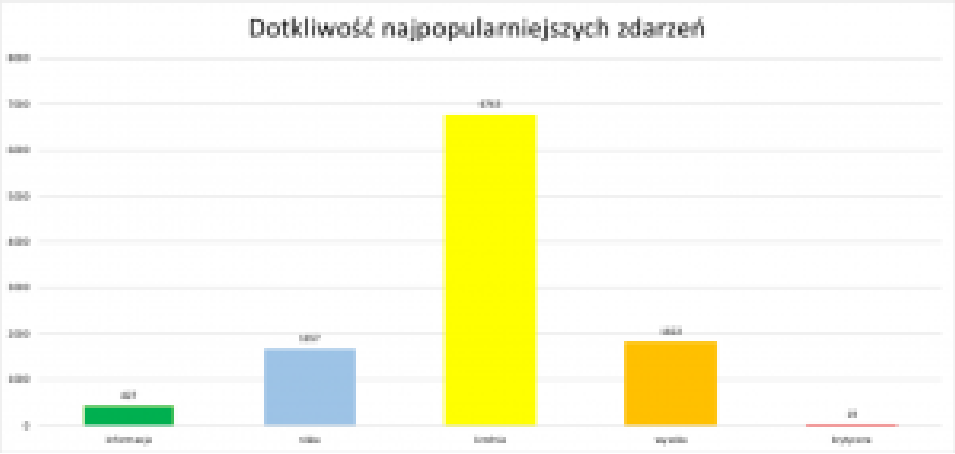
Tab. nr 3 Typy zdarzeń oraz ich liczba w styczniu

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.

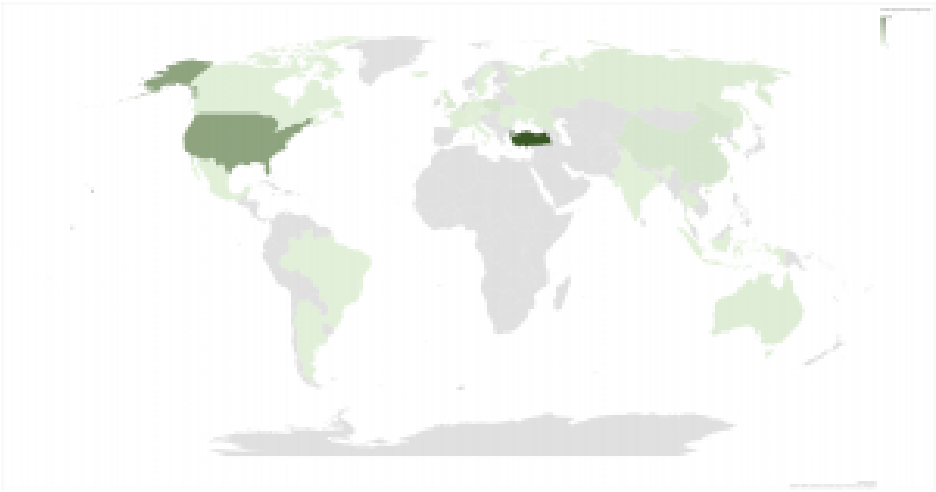
Na poniższym wykresie przedstawiliśmy potencjalną dotkliwość najpopularniejszych zdarzeń występujących w badanym okresie.



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 419 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

Największą bolączką każdego administratora serwerów jest spam. Jako użytkownicy przywykliśmy do niego na tyle, by traktować go jako rozrywkę do czytania czy też po prostu całkowicie ignorujemy folder, do którego takie wiadomości wpadają. Jednakże spam to nie tylko niechciane oferty handlowe. W dużej mierze okazuje się być pierwszym etapem „niezamówionych testów penetracyjnych" albo też po prostu próbą okradzenia nas z tego co mamy najcenniejsze – naszych danych. O phishingu pisaliśmy już wcześniej, więc zachęcamy do zapoznania się z artykułem na ten temat.

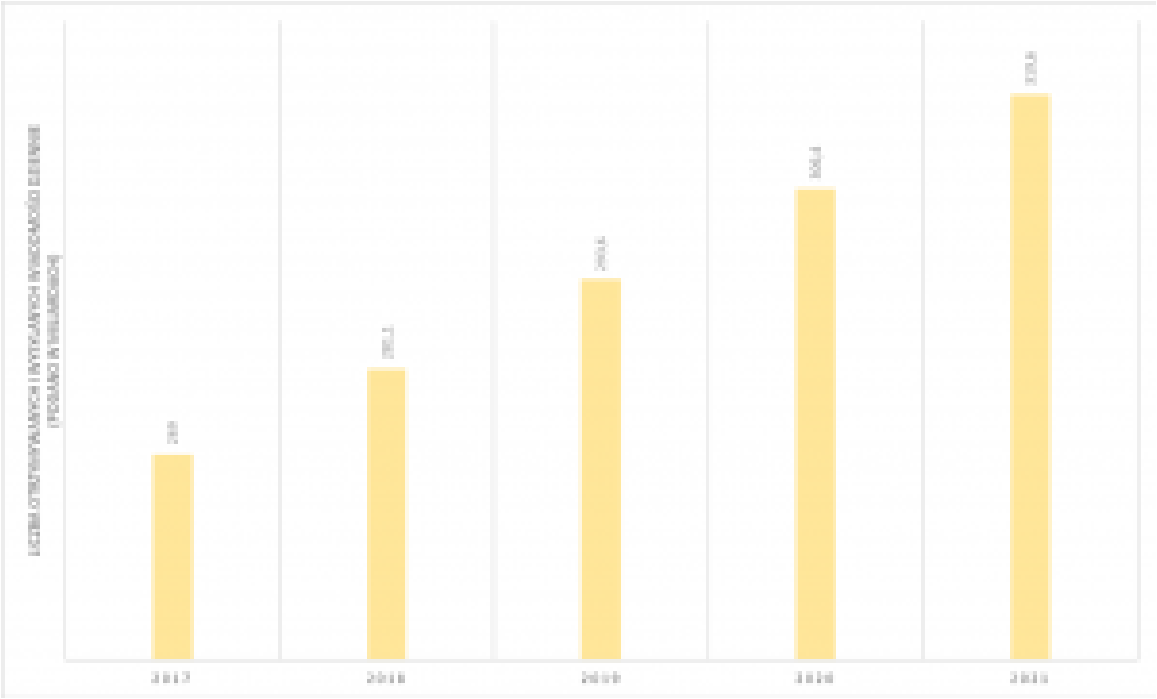
W 2013 Danny Hillis podczas konferencji „Ted" swoją prezentację zaczął od poniższych słów:

> Książka, którą trzymam w ręce to spis wszystkich osób, które posiadały adres e-mail w roku 1982. (Śmiech) Tylko wydaje się duża. Na każdej stronie jest około

20 osób, ponieważ mamy tu imię, adres oraz numer telefonu każdej z nich. Każdy jest wymieniony podwójnie, osobno z imienia i adresu email. To bardzo mała społeczność. Wtedy w Internecie istniały tylko dwie inne osoby o imieniu Danny, znałem obydwie. Nie znaliśmy się wszyscy, ale w pewien sposób ufaliśmy sobie i ten rodzaj zaufania rozprzestrzenił się na całą sieć i istniało prawdziwe poczucie, że mogliśmy w na sobie polegać.

Całą prezentację z polską transkrypcją możecie obejrzeć klikając w ten link.

Dzisiaj e-maile są jednym z najlepszych i najczęściej wykorzystywanych wektorów ataku. Łatwo domyślić się dlaczego – obecnie to główny kanał komunikacyjny w Internecie, a liczba dziennie wysyłanych i otrzymywanych wiadomości dawno przekroczyła setki miliardów. Na początek trochę statystyk odnośnie samych wiadomości. żebyście mogli zobaczyć skalę o jakiej mówimy.



Jak wspomnieliśmy liczby te dawno przekroczyły setki miliardów. Najnowsze prognozy natomiast przewidują, że do 2021 roku liczba dziennie wysyłanych i odbieranych maili osiągnie zawrotną wartość prawie 320 miliardów.

Najczęściej jesteśmy pytani jak duża jest skala problemu. Możemy jedynie ujawnić ze serwer o nazwie operacyjnej „Ichibanme" odbiera miesięcznie około 20-30 tysięcy wiadomości o charakterze spamu. Dziś postanowiliśmy opisać naszego ulubionego spamera. Od kilku miesięcy otrzymujemy – zapewne nie tylko my – wiadomości na pozór dostarczające nam reklamy.

Na koniec ciekawostka, czyli trolling jaki przygotowaliśmy dla naszych najbardziej wytrwałych i skrupulatnych spamerów. Jako, że PHT znany jest z czarnego poczucia humoru, mamy dla spamerów specjalną wiadomość zaszytą w komunikatach serwerowych. Na każdą wiadomość z niezwykle dużą ilością spam punktów odpowiadamy komunikatem opatrzonym linkiem do fragmentu serialu Silicon Valley, mianowicie do momentu, gdy Gilfoy wygłasza najbardziej charakterystyczne dla swojej postaci słowa:

Dlaczego postanowiliśmy akurat teraz wspomnieć o zjawisku jakim jest spam? Kiedyś już pht popełnił analizę jednego przypadku spamowego, [możecie znaleźć go na naszym blogu ,](#) więc tym razem tego Wam oszczędzimy. Studium obecnego przypadku pokazało nam, że za obecną ilością dziesiątek tysięcy maili, które do nas docierają stoi jedna firma

zajmująca się marketingiem email. Nie chcemy wskazywać ani IP ani nazw firm palcem – może po prostu niechcący się zapętlili…

Ciekawostka na koniec – wszystkie maile przychodzą na cztery konkretne adresy:

- piotr.jasiek@s-m-s.pl
- piotr.jasie@s-m-s.pl
- pht@s-m-s.pl
- info@s-m-s.pl

O ile w randomizowany spam na info@ jeszcze byśmy uwierzyli, to już w to, że wiadomości przypadkowo trafiają nam na maile, które nie istnieją i nie są nigdzie podawane (pht@) już nie uwierzymy. Przyznać się świntuszki, kto postanowił sprzedać nam trochę malware razem z latarką?

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