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

Spis treści

Wstęp

Przygotowaliśmy dla Was piąty 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 wydaniach badaniu poddane zostały dane zebrane z własnych narzędzi służących do administrowania ruchem do serwerów. Przeanalizowaliśmy dane za okres od 01.02.2020 do 29.02.2020. 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 dalszym ciągu 2020 nas zaskakuje pod względem liczby zdarzeń. W badanym okresie odnotowaliśmy 54.049 prób ingerencji w nasze systemy, co oznacza, że liczba ta wzrosła prawie pięciokrotnie w porównaniu do poprzedniego miesiąca. Średnia liczba zagrożeń w tym miesiącu wyniosła ponad 1.8 tysiąca zdarzeń dziennie. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w lutym

W lutym ponownie liczba prób kompromitacji naszych serwerów utrzymywała się średnio na stałym poziomie. Wykres jest natomiast bardzo płaski ze względu na bardzo duży skok liczby prób kompromitacji w jednym dniu poprzedniego miesiąca. Oczywistym więc jest, że nasze zainteresowanie podczas przygotowywanie publikacji zdecydowanie przykuł 16.02.2020. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – w sumie 46.977

zdarzeń. Poniżej prezentujemy tabele, w których przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	Liczba zdarzeń
SIP INVITE Method Request Flood Attempt	46906
UNIX Portmapper Remote Infomation Retrieving Attempt	37
HTTP Non RFC-Compliant Response Found	10
FTP: login Brute-force attempt	8
ZmEu Scanner Detection	6
HTTP OPTIONS Method	4
DistCC Daemon Command Execution	2
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	2
HTTP Directory Traversal Vulnerability	1
MailEnable IMAP Server Long Tag anomaly	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 16.02.2020 r.

Skąd tak duża liczba zdarzeń? Ma to bezpośredni związek z uruchomieniem przez naszego Prezesa telefonii VoIP, której "premiera" przypada na 16 lutego. Zakładamy więc, że w związku z tym w dniu nasz firewall przyjął najwięcej ataków typu SIP INVITE Method Request Flood Attempt, bo aż 46.906. Jest to ogromna liczba biorąc pod uwagę, że przez cały okres publikacji biuletynów łączny ruch ze wszystkich podatności na naszym firewallu wynosił lekko ponad 25 tysięcy incydentów. Zdecydowanie zainteresowało nas to zdarzenie oraz zdominowało lutowe zestawienie najczęściej występujących zagrożeń, więc w część techniczną tego wydania poświęcimy na analizę tego typu zdarzeń.

Przedstawiamy Wam też nasz Top 20, czyli listę najbardziej popularnych zagrożeń w lutym. 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
SIP INVITE Method Request Flood Attempt	46906
HTTP SQL Injection Attempt	2079
UNIX Portmapper Remote Infomation Retrieving Attempt	1526
HTTP Directory Traversal Vulnerability	779
Microsoft Windows win.ini access attempt	747
FTP: login Brute-force attempt	497
HTTP Non RFC-Compliant Response Found	473
ZmEu Scanner Detection	379
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	207
HTTP OPTIONS Method	110
HTTP Unauthorized Brute-force Attack	81
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	55
Bash Remote Code Execution Vulnerability	49
MS-RDP Brute-force Attempt	33
MAIL: User Login Brute-force Attempt	23
HTTP /etc/passwd Access Attempt	18
DistCC Daemon Command Execution	14
MailEnable IMAP Server Long Tag anomaly	12
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	10
Invalid HTTP Version Found	8

Tab. nr 3 Typy zdarzeń oraz ich liczba w lutym

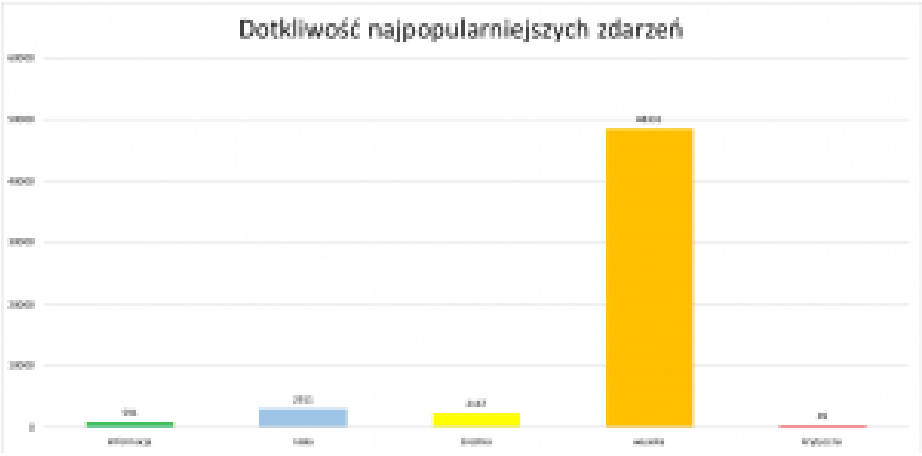
Wyżej wspominamy o pojęciu potencjalnej dotkliwości zdarzenia. Jak sama nazwa wskazuje jest to szacowany zakres szkód jakie może wyrządzić dana podatność w naszej infrastrukturze o ile dojdzie do jej pomyślnego wykorzystania. Samą dotkliwość można podzielić na 5 różnych poziomów:

- 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 653 unikalnych adresów IP wraz z ich krajem pochodzenia. Tym samym udało nam się zidentyfikować 34 kraje, 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

W jaki sposób można by nazwać firmę świadczącą usługi w głównej mierze przez internet bez sprawnie działającego BOK-u? Umówmy się, że na czas czytania tego wpisu wszyscy zapominamy o tych dziesiątkach minut spędzonych na słuchaniu melodyjki danego operatora w oczekiwaniu na połączenie z konsultantem. Przenosimy się do alternatywnej rzeczywistości, gdzie wszystko możemy załatwić od ręki po pierwszym sygnale w słuchawce.

Odpowiedzmy sobie w takim razie na pytanie zadane powyżej. Co sobie myślimy o firmie, w której swoją sprawę możemy załatwić jedynie drogą e-mail i to bez pewności, że otrzymamy odpowiedź? My jako zespół S.M.S. jednogłośnie uznalibyśmy takiego usługodawcę/sprzedawcę za mało profesjonalnego. Dodatkowo możliwość kontaktu telefonicznego z firmą poprzez może stanowić dla konsumenta kolejny z etapów sprawdzenia, czy dany przedsiębiorca jest wiarogodny. Niejako z tematem infolinii wiąże się omawiana dzisiaj podatność jaką nasz firewall określa mianem „SIP INVITE Method Request Flood Attempt".

Żeby lepiej zrozumieć o co tutaj chodzi warto zacząć od samego początku. Czym jest ten cały SIP?

SIP, czyli Session Initiation Protocol jest protokołem, który powstał w piwnicy chłopaków

z Internet Engineering Task Force. Dzięki niemu możliwe jest zestawienie sesji pomiędzy wieloma klientami. Za sprawą tego, że jest bardzo prosty i elastyczny (co jest uważane za największą zaletę tego protokołu) wygryzł rozbudowany standard H.323 i stał się dominującym protokołem sygnalizującym telefonii IP.

SIP opiera się o architekturę typu klient-serwer i wykorzystuje w sobie protokoły http i SMTP. SIP realizuje usługę, która nosi nazwę sesji. Oznacza to, że musi on najpierw utworzyć sesję oraz zarządzać nią przez cały okres trwania. Sesja jest to w skrócie uporządkowana wymiana danych pomiędzy dwoma lub więcej urządzeniami. Dosyć ciekawym elementem są dwa ostatnie słowa. "Więcej urządzeń" oznacza w praktyce, że poza możliwością prowadzenia konferencji istnieje także opcja łatwego podsłuchiwania waszych rozmów.

Żeby nie było zbyt kolorowo, SIP ma też swoje wady. Przez to, że użytkownicy nie zawsze realizują połączenia z tego samego miejsca, wymagane jest dołączenie funkcji śledzenia użytkownika. Drugim, trochę większym problemem jest fakt, że użytkownicy mogą korzystać zarówno z komunikacji tekstowej jak i głosowej czy wideo. Używanie powyższych mediów powoduje, że dla każdego z nich są inne wymagania co do przepustowości czy opóźnień.

W tym miejscu zakończymy rozważania o samym protokole i przejdziemy do podatności która wiąże się z ostatnim wspomnianym problemem. SIP Register Flood (bo tak prawidłowo nazywa się to działanie) jest atakiem warstwy aplikacji na nasz wspaniały protokół SIP. Polega on na wykorzystaniu podatności na bezproblemowe przyjmowanie pingowania, co w efekcie prowadzi do zalania naszego systemu VoIP różnymi komunikatami ping lub komunikatami połączeń, takimi jak SIP INFO, NOTIFY itp. Ma to na celu wyczerpanie przepustowości i zasobów.

Co to oznacza w praktyce? Na pewno nie raz znaleźliście się w sytuacji, kiedy grając w wasze ukochane MMO lub FPS najpierw zobaczyliście szary ekran, a po chwili dopiero jego powód. Miało to związek z wysokim pingiem. Bardzo analogicznie ma się sprawa z rozmowami np. telefonicznymi podczas tego ataku. Prowadzi to do najprościej mówiąc bałaganu, gdzie wy mówicie swoje, a osoba po drugiej stronie słuchawki odpowiada zupełnie coś innego lub w najgorszym wypadku nie możecie nawet połączyć się ze sobą.

Kolejnym atakiem który zawiera się w tej nazwie jest sytuacja wszystkim bardzo dobrze znana po części z Facebooka, po części z mediów. Paradoksalnie są na niego narażeni nie seniorzy, a osoby roztargnione lub biznesmeni. Pamiętacie te nieodebrane połączenia z kierunkowego (+225) wykonywane zazwyczaj wieczorem lub w nocy? Dokładnie, to wcale nie są przypadkowe połączenia z Warszawy jak może sugerować kierunkowy, a wprost

z Wybrzeża Kości Słoniowej. Tak samo przypadkowa nie jest godzina ich wykonywania. Połączenia te wykonywane są przez skrypty, które włamują się do niezabezpieczonych centralek VoIP. Jeżeli taka centralka jest podatna, w łatwy sposób można podrobić Caller-ID i w efekcie podmienić numer dzwoniącego na dowolny wybrany przez atakującego. Zazwyczaj działanie takie podyktowane jest chęcią zysku. Stawki płacone sobie wzajemnie przez operatorów telekomunikacyjnych są bardzo łakomym kąskiem dla potencjalnych atakujących.

Przedstawmy teraz w telegraficznym skrócie cały przebieg działania tego typu:

1. Atakujący dostaje się do bramki VoIP i podmienia Caller-ID na numer z kierunkowym (+243) czyli Republiki Konga.
2. Skrypt wykonuje z tej bramki połączenia w późnych godzinach wieczornych lub w nocy do potencjalnych ofiar puszczając im jeden ”sygnał”.
3. Ofiara po śniadaniu sięga po telefon i sprawdza nieodebrane połączenia. Numer łudząco przypomina kierunkowy z Płocka (24) więc oddzwania.
4. Połączenie wykonywane jest na numer podmieniony, ten który wyświetlił się naszemu panu roztargnionemu na ekranie po przebudzeniu.
5. Podczas rozmowy licznik u operatora się kręci, co w efekcie ofiara odczuje na rachunku telefonicznym pod rubryczką ”Połączenia międzynarodowe”.

Ciekawostką jest pewien trick stosowany przez atakujących. Polega on na zasymulowaniu dźwięku zakończenia połączenia. Potencjalna ofiara może nie spojrzeć na ekran telefonu po usłyszeniu tego sygnału, co przedłuży jeszcze minimum o parenaście sekund cały proces naliczania opłat.

Nie od dziś wiadomo, że lepiej jest zapobiegać niż leczyć. Jak się w takim razie bronić przed atakami wymienionymi powyżej? Dróg jest kilka.

- Oczywiście jednym z najlepszych rozwiązań jest zajrzenie do dokumentacji i zaleceń producenta dostarczającego rozwiązań, których używamy w naszej sieci. Nie ma sensu rozwijać tego podpunktu. Z reguły producent (w tym przypadku infrastruktury VoIP) najlepiej zna wszystkie bolączki swojego systemu.
- Kolejnym bardzo dobrym rozwiązaniem jest używanie narzędzi wykrywających urządzenia, które wykazują cechy tzw. skanerów. Skanery wykonują wiele prób wysłania żądań do SIP w krótkim przedziale czasu. Tak na logikę, chyba nie jest fizycznie wykonalne ręczne wysyłanie żądania w równych odstępach co kilkadziesiąt milisekund, prawda?
- Używanie autoryzacji i uwierzytelniania też może być jakimś pomysłem. Jest to kolejne

działanie zapobiegające, jednak nie gwarantuje ono bezpieczeństwa w stu procentach. Niestety w tej metodzie wykorzystywane jest archaiczne już szyfrowanie MD5, aczkolwiek lepsze to niż nic.
- Następnym, już trochę lepszym rozwiązaniem jest blokada odpowiednich portów na Firewallu. Odmowa dostępu na port 5060/UDP skutecznie uniemożliwi dostanie się adresów niepowołanych do naszej bramki.

Podsumowanie

W tym miesiącu przytoczyliśmy przykład podatności, której głównym zadaniem jest przeciążenie systemu VoIP firmy skutecznie wpływając na zmniejszenie jego przepustowości jak również zasobów. Może się wydawać, iż znów wskazaliśmy podatność, trywialną i prostą. Powiązana jest ona jedynie ze złym skonfigurowaniem usługi. Jednak jej następstwa mogą zagrozić pod kątem finansowym zarówno firmie jak i osobom trzecim. Jak widać po analizie statystycznej bowiem uruchomienie telefonii VoIP łączy się ze wzmożonym występowaniem tej podatności. Z tego względu drodzy administratorzy VoIP’owych rozwiązań serdecznie zachęcamy Was do sprawdzenia swoich konfiguracji i w razie potrzeby naniesienia koniecznych zmian. Nie jest to zadanie praco czy czasochłonne, a w ten sposób oszczędzicie sobie wielu problemów w przyszłości.

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