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

Spis treści

Wstęp

Przygotowaliśmy dla Was trzeci numer naszego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte” analizujący zagrożenia 2019 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.

Na pewno przyzwyczailiście się do tego, że biuletyny pojawiają się na początku miesiąca. Bijemy się w pierś i przyznajemy – w tym roku będzie tak samo. Jednak biuletyn grudniowy miał lekką obsuwkę ze względu na ilość pracy jaka zaskoczyła nas po okresie świątecznym. Bardzo Was przepraszamy i obiecujemy poprawę w przyszłych miesiącach.

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.

W grudniowym wydaniu biuletynu, podobnie jak w zeszłym miesiącu, badaniu poddane zostały dane zebrane z własnych narzędzi służących do administrowania ruchem do serwerów. Przeanalizowaliśmy dane za okres od 01.12.2019 do 31.11.2019. 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 analizowanym okresie czasu nasze systemy wykryły przeszło 5.2 tysiąca prób ingerencji w naszą sieć. Natomiast dziennie dochodziło średnio do 165 potencjalnych zagrożeń. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w grudniu

W grudniu liczba prób kompromitacji naszych serwerów utrzymywała się średnio na stałym poziomie. Nasze zainteresowanie przykuł szczególnie 13.12.2019. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – w sumie 966 zagrożeń. Poniżej prezentujemy tabelę, w której przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	Liczba zdarzeń
HTTP SQL Injection Attempt	884
UNIX Portmapper Remote Infomation Retrieving Attempt	32
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	30
HTTP Non RFC-Compliant Response Found	15
MailEnable IMAP Server Long Tag anomaly	2
HTTP Directory Traversal Vulnerability	1
AWStats Remote Code Execution Vulnerability	1
Spreecommerce Arbitrary Command Execution Vulnerability	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn.
13.12.2019 r.

Przedstawiamy Wam też nasz Top 20 zagrożeń w grudniu. 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
HTTP SQL Injection Attempt	1994
UNIX Portmapper Remote Infomation Retrieving Attempt	1100
FTP: login Brute-force attempt	690
HTTP Non RFC-Compliant Response Found	389
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	375
ZmEu Scanner Detection	320
HTTP Unauthorized Brute-force Attack	99
HTTP Directory Traversal Vulnerability	50
HTTP OPTIONS Method	43
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	35
HTTP /etc/passwd access attempt	16
Invalid HTTP Version Found	15
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	14
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	14
Bash Remote Code Execution Vulnerability	10
MailEnable IMAP Server Long Tag anomaly	8
JavaScript Obfuscation Detected	8
Snort URIContent Rules Detection Evasion Vulnerability	7
AWStats Remote Code Execution Vulnerability	7
Microsoft ASP.NET Path Validation Security Bypass Vulnerability	6

Tab. nr 2 Typy zdarzenie oraz ich liczba w grudniu

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.

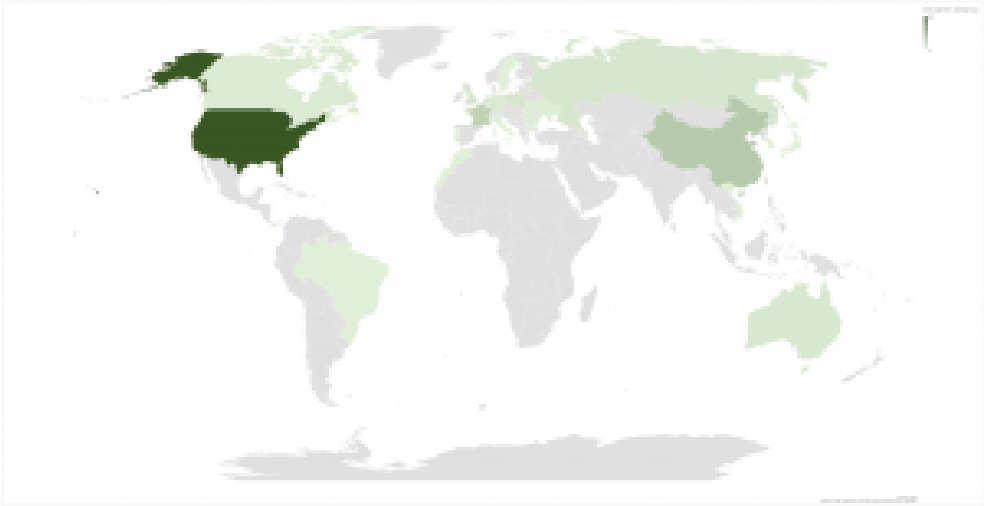
- Wysoka – zagrożenie, które potencjalnie może stać się krytycznym, jednak dzięki występowaniu czynników łagodzących nie jest możliwa jego eskalacja. Do kategorii zagrożeń poziomu wysokiego można zaliczyć zagrożenia, które są trudne do wykorzystania, nie dają podwyższonych uprawnień lub są w stanie dotknąć 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 209 unikalnych adresów IP wraz z ich

krajem pochodzenia. Tym samym udało nam się zidentyfikować 23 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.



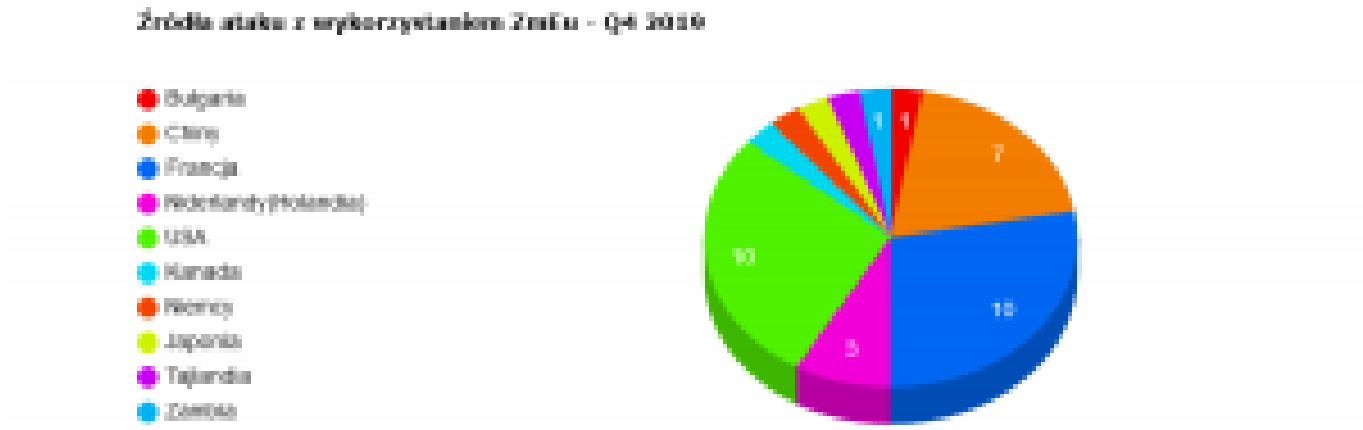
Mapa nr 1 Kraje próbujące atakować infrastrukturę S.M.S. w badanym okresie.

Analiza przypadku wybranych zgłoszeń

Lubicie opowieści fantastyczne? Więc na pewno znacie smoka z pierwszej ekranizacji Wiedźmina czy smoki z Gry o tron, ale czy wiecie cokolwiek o „Zmeu”? Zapewne nie. Tym razem w naszym biuletynie postanowiliśmy opowiedzieć Wam o pewnym rumuńskim skanerze podatności. Dlaczego akurat o nim? Bardzo często pojawia się w naszych logach.

Dla przykładu w samym grudniu odnotowaliśmy ruch z pięciu krajów. Poniższy wykres przedstawia ilość źródeł (adresów IP) podzielonych na kraje:

Jeżeli spojrzeć na ostatni kwartał roku 2019 otrzymamy podobny, aczkolwiek poszerzony stosunek krajów:



Na początek warto opowiedzieć skąd wzięła się nazwa skanera. Warto zerknąć do Wikipedii.

Zmeu – istota z rumuńskiej mitologii ludowej i baśni. Wyobrażany w postaci antropomorficznej z pewnymi cechami gadzimi, takimi jak ogon i ciało pokryte łuskami. W mitologii ludowej związany jest z żywiołem powietrza i zjawiskami atmosferycznymi,

takimi jak gwałtowne burze. Często utożsamia się go wtedy ze smokiem (rum. *balaur*). W bajkach jest zwykle przeciwnikiem bohatera o imieniu Făt-Frumos, porywaczem kobiet, posiada nadludzką siłę, własny pałac, często jeździ konno i posługuje się buławą. Jego nazwa jest prawdopodobnie zapożyczeniem z języków słowiańskich, wywodzi się od słowa **zmьjь* (zmij) oznaczającego Żmija. Podobne postacie znane są także w folklorze Bułgarów i Rosjan pod nazwą *змей* (zmej).

Jak widzicie, hakerzy lubią finezje i polot. I to też doceniamy. Nazwanie oprogramowania do przeprowadzania bardziej lub mniej zamówionych testów penetracyjnych imieniem potwora, opisem zakrawającego na samego diabła ma zapewne sugerować potężne działanie powyższego oprogramowania. Sami to zrobiliśmy, ale po kolei.

W Internecie można znaleźć wiele opisów użycia/znalezienia w swoich logach przypadków zastosowania oprogramowania o nazwie ZmEu. Zostawia ono w logach niezwykle charakterystyczne ślady. Schemat działania jest prosty. Najpierw robak skanuje porty szukając znanych sobie podatności takich jak dziurawy phpmyadmin, a gdy je znajdzie umieszcza na serwerze backdoor za pomocą którego można później z łatwością dostać się na zainfekowany serwer. Poniżej przykładowy fragment ruchu nagrany podczas pojawienia się ZmEu w naszej sieci.

```
GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: ZmEu
Host: 79.137.31.32
Connection: Close
```

Gdybyście szukali kiedyś aktywności tego robaka w swoich logach w 99% przypadków należy szukać wartości pola user-agent – „ZmEu"

W historii znane jest kilka przypadków, gdy Zmeu został wykorzystany do akcji hakerskich bardziej zaawansowanych niż zautomatyzowany atak botnetu serwowany przez serwer CNC oparty o protokół IRC. O to kilka przykładów zastosowania tego oprogramowania.

W 2011 roku hakerzy skompromitowali serwer Massachusetts Institute of Technology (MIT), dzięki czemu posłużył im on jako narzędzie do przeprowadzania ataków, a także skaner do wyszukiwania luk bezpieczeństwa czy podatności. W wyniku przeprowadzonych działań z użyciem zhakowanej maszyny doszło do naruszenia około 100 000 domen.

Odnotowano również, że oprogramowanie ZmEu wykorzystywane zostało podczas ataków malware. Ataki te polegały na łamaniu haseł SSH z ciągłą infekcją złośliwym oprogramowaniem typu backdoor. Pierwsze tego typu ataki odnotowano w 2012 roku, a ich popularność niezmiennie rośnie.

Natomiast w 2013 roku firma Fortinet wydała raport z badań nad krajobrazem zagrożeń *FortiGuard* od 1 października do 31 grudnia 2012 r. Badanie wskazuje kilka interesujących faktów na temat zarabiania pieniędzy na szkodliwym oprogramowaniu oraz narzędziach używanych przez hakerów w ostatnim kwartale 2012 r. Firma podczas analiz zagrożeń w badanym okresie wykryła wysoki poziom aktywności przy użyciu oprogramowania ZmEu, które z powodzeniem było wykorzystywane do określania, które serwery są podatne na ataki. Według firmy poziomy aktywności wzrosły dziewięciokrotnie między wrześniem a grudniem 2012 r. Jak zaznacza Fortinent wzrost tego typu aktywności spowodowany jest zwiększonym zainteresowaniem ze strony grup hacktywistycznych w takich działaniach jak protesty czy wsparcie dla ruchów aktywistycznych na całym świecie.

Podsumowanie

Biorąc pod uwagę dane przedstawione powyżej ponownie zauważamy jak istotny jest stały monitoring aktywności w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci. Bez znaczenia ma wielkość czy skala działalności, incydenty bezpieczeństwa w dzisiejszych czasach dotyczą każdego – od użytkownika końcowego, przez małe przedsiębiorstwa, a na dużych korporacjach kończąc. Z tego względu tak istotny jest właściwy poziom usług z zakresu bezpieczeństwa IT. W tym miejscu warto również dodać, że mimo tak licznych zdarzeń i prób exploitacji (tj. wykorzystania błędów lub luk w oprogramowaniu/systemie/aplikacji itp.) naszego systemu, dzięki stałemu monitoringowi oraz prawidłowo zabezpieczonej infrastrukturze żadna podatność nie miała wpływu na ciągłość działania naszej organizacji ani w żadnym stopnia nie wpłynęła na jakość świadczonej usługi.

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