Dzisiaj mam dla was długo zapowiadane podsumowanie tegorocznej edycji B-Sides. Miało być w ciągu tygodnia – jest miesiąc. Dlaczego? Po konferencji spotkał mnie nawał zadań, kilka projektów wręcz wyrosło jak grzyby po deszcze i byłem zmuszony przyłożyć swoje dłonie do klawiatury po to by na tych projektach generować profity i podsumowanie B-Sides gdzieś mi umknęło na boku. Tym samym, chyba pierwszy raz odkąd ten blog istnieje, a jest to już prawie rok, pragnę przypomnieć/uświadomić wszystkim, którzy czytają moje artykuły, że robię go tak naprawdę w formie wolontariatu, nie zamierzam wstawiać tu innych reklam niż te, polegających na zalinkowaniu fajnego bloga technicznego czy kilku słów o serwerowni z której korzystam. W tym blogu, nie chodzi o profity, a przede wszystkim o podzielenie się wiedzą – tym co wiem na pewno, oraz moimi opiniami i labami, które robię z czystej ciekawości. Mija rok od założenia bloga, mamy już stałych czytelników, zastanawiałem się nad zorganizowaniem możliwości „datku”/”darowizny” na utrzymanie serwera czy też domeny, pozostawiam tę sprawę otwartą, na pewno ten temat jeszcze powróci. Tym czasem zapraszam do dalszego czytania!

W tym artykule, który tak naprawdę jest czymś w rodzaju mojego pamiętnika z konferencji, chcę przede wszystkim opowiedzieć o masakrycznej ilości pracy włożonej przez organizatorów, których można by policzyć na palcach jednej ręki, może dwóch. Przypomnieć zaangażowanie ludzi z PM bez których, pewnie impreza by się nie odbyła, ujawnić wszystkie sekretne sekrety oraz opowiedzieć historię tego eventu widzianą z mojego punktu widzenia – z punktu widzenia admina sieci. Nie ma co się oszukiwać. Zazwyczaj event tak naprawdę zaczyna się kilka miesięcy przed oficjalnym „Event uważam za otwarty”. Związane jest to z dużą ilością przygotowań, które są konieczne do tego by podczas konferencji organizatorzy mogli siedzieć i cieszyć się zasłużonym fejmem. Ale! Wszystko w odpowiedniej kolejności.

Dla mnie B-Sides zaczęło się tak naprawdę w wieczór poprzedzający event. Wtedy też do Warszawy przyjechał ostatni z organizatorów. Po odebraniu Xaxesa udaliśmy się do mojego mieszkania dalej zwanego „pehatspejsem” i zabraliśmy się za przygotowywanie sieci na konferencję. Praktycznie do ostatniego momentu wierzyliśmy, iż uda się nam załatwić wersje hardware PaloAlto. Niestety udało się nam załatwić tylko wirtualna maszynę, ale i z tym daliśmy sobie radę.

 Przygotowaniom sieci towarzyszyła prawdziwa burza mózgów jakiej nie powstydziło by się niejedno korpo pokroju FB, M$ czy

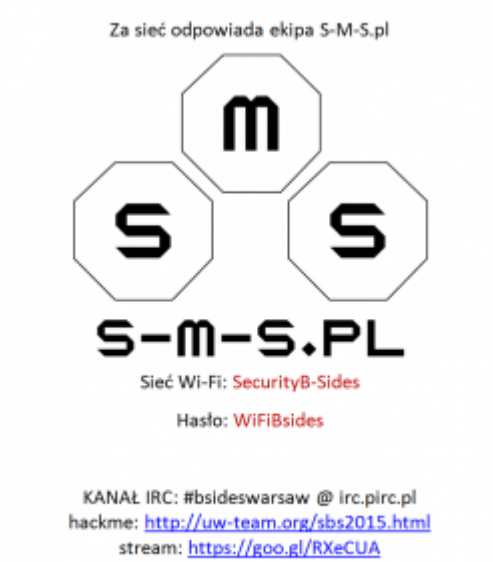
 Jabłuszko. Każdy pojawiający się problem razem z Xaxesem rozwiązywaliśmy w sprawny, aczkolwiek nie do końca konwencjonalny sposób, tak też między innymi narodziła się idea switcha najnowszej generacji opartego na hubie usb i chińskich przejściówkach usb-ethernet. Konstrukcja miała sens i nawet względnie działała zapewniając bezpieczne łącze internetowe… No dobra, może i rozdawała tylko adresy IP i o dziwo innych pakietów niż requesty dhcp nie dało sie przesłać przez nie, ale to już inna historia, jestem pewien, że kiedyś wrócę do tego projektu i zobaczymy co uda się przerobić na switch ;).

Oczywiście gdybym pominął kwestie żywieniowe, pewnie pominął bym jedną z istotniejszych kwestii przygotowań przed konferencyjnych. Z racji tego, iż Xaxesa odebrałem około godziny 22 i od razu zabraliśmy się za przygotowania jakoś około godziny pierwszej, może drugiej zrobiliśmy się nieco głodni. Tutaj narodziło się pewne sformowanie, które

zapamiętam z pewnością… „Xaxes lubi krwiste” i chodzi oczywiście o karkówkę którą smażyliśmy o owej późnej nocnej godzinie, swoją drogą, podziwiam swoich współlokatorów za ich cierpliwość.

Po kilku godzinach kombinacji i nauki (dla Xaxesa było to pierwsze spotkanie z technologią PaloAlto, więc musiałem odkazić go z wiedzy zdobytej w szkole dotyczącej Cisco i wbić do głowy trochę inne myślenie) w końcu Xaxesowi udało się zasnąć, ja półspiąc i oglądając na yt filmy o ufo doczekałem rana.

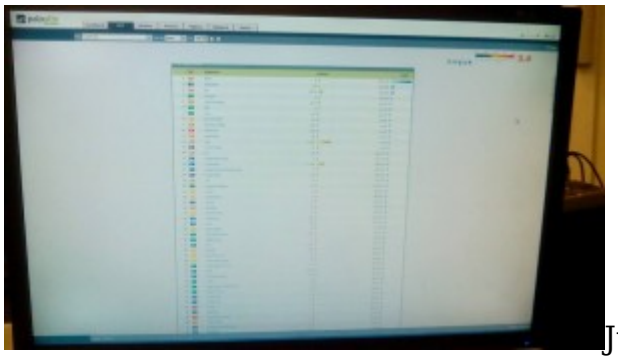
„Kolejny” a właściwie pierwszy oficjalny dzień B-Sides zaczęliśmy od porannej kawy, spakowania sprzętu do walizki, ogarnięcia się i dotarcia do Państwa Miasta gdzie organizowana była tegoroczna edycja B-Sides. W tym miejscu chcę gorąco podziękować ludziom z PM (Wiktorowi Jędrzejewskiemu oraz Ewelinie Kycia) za pomoc w ogarnięciu kilku małych ale istotnych kwestii (przedłużacz czy zaciskarka) bez których postawienie sieci trwało by dłużej niż zakładały najczarniejsze scenariusze. W tym momencie warto by wspomnieć z czego zbudowaliśmy sieć. Zbudowaliśmy ją dosyć prosto i działała bez większych problemów – wnioski na przyszłość? Zdecydowanie potrzebny wydajniejszy AP.



Zaprojektowana i zbudowana przeze mnie i Xaxesa sieć, którą wykorzystaliśmy podczas SBS była bliźniaczo podobno projektu „Yuuki” o którym, mam nadzieję, wstawię pełen artykuł.  Za bramę oraz firewall służyła nam wirtualna wersja PaloAlto VM-300, które pozwoliło nam zebrać istotne informacje czy też zbalansować utylizacje sieci. Pierwszy dzień, prócz porannego stresu związanego z uruchomieniem sieci oraz dostosowaniem polityk bezpieczeństwa minął dla mnie jako admina całkiem spokojnie. Nie będę się rozpisywał, która z prezentacji była dla mnie najciekawsza, niejednokrotnie w czasie prezentacji byłem wyrywany z transu spowodowanego prelekcją przez brzydko wyglądające logi z palo (tak, abuserzy też nie omieszkali nas odwiedzić).

Z pierwszego dnia dla mnie osobiście poza głównym nurtem konferencji największym, a zarazem przyjemniejszym były trzy momenty. Osoby, które przyszły jeszcze przed dziewiątą – swoją drogą w tym miejscu serdecznie pozdrawiam osobę, która przyszła do „stanowiska adminów” z rozpiską z tamtego roku i twierdziła, że od dziewiątej mamy pierwsze prelekcje – miały okazję widzieć historyczny moment w którym to wraz z nikowem podajemy sobie dłonie na znak pokoju. Drugim momentem, właściwie wydarzeniem, które się powtarzało przez kolejne trzy dni konferencji była miła obsługa PM, a właściwie

to kelnerki, które to cały dzień z uśmiechem na twarzy podawały nam „americane”, no i oczywiście świetne jedzenie. Trzeci moment? Trzeci moment stał się już właściwie legendą, było to gdy Gaweł Mikołajczyk sformułował swoja wypowiedź w taki sposób, iż brzmiała „Cisco na dzień dobry daje klientowi ra(c)ka”. Gaweł miał też okazję do strollowania mnie i trafnie ją wykorzystał. W czasie między jego prezentacją a afterparty rozmawiałem z jednym z słuchaczy przy wyjściu z PM, oczywiście dumny z posiadanego napisu na koszulce, który głosił iż jestem inżynierem wdrażającym PaloAlto inaczej mówiąc posiadaczem certyfikatu ACE. Gaweł, pracownik Cisco, trzymając na rękach dziecko powiedział kolejny złoty tekst który powinien być kolejnym hitem tak jak ten o raku. Brzmiało to mniej więcej tak: „Zrób Panu papa bo ma fajną koszulkę”. Nie miałem okazji wydukać z siebie czegoś więcej niż zwykłe „dzięki” ale… Gaweł! Wiem, że koszulka fajna, szkoda że uciekłeś, zaproponowałbym wymianę koszulek.

 Już po pierwszym dniu mieliśmy sporo materiału do analizowania, pojawiły się pierwsze alerty jak i pierwsze kwiatki takie jak duże ilości dziwnego, nieznanego dla palo ruchu udp/tcp (pełna lista na koniec artykułu).
Tak na marginesie chcę zaznaczyć, że czasami, nie zawsze ale się zdarza iż pod takim ruchem kryje się złośliwe oprogramowanie. Dla bezpieczeństwa taki ruch został po prostu wycięty. Nie ingerowaliśmy za to w aplikacje szyfrowane za pomocą SSL, nie mniej jeśli został wykryty ruch SSL do proxy – był on wycinany. Tutaj ukłony w stronę Michała Trojnary i jego „stunel’a„. Ów „stunnel” był widziany przez palo jako ruch ssl. To co spowodowało, iż ten ruch mnie zaciekawił to wysoki port na który szedł ruch. Sprawdziłem ip na który ruch wędrował i natrafiłem na stronę Michała na której wspomina i linkuje stunel. Przygotowując się do konferencji, założyłem, że nie tylko zastosuje QOS, aby zapewnić priorytet transmisji live z konferencji, ale też uniemożliwię korzystanie z TOR’a, proxy, wszelakiej maści VPN’ów i wszystkiego co mogło by wysycać łącze. To co zostało zablokowane mieści się na poniższej liście:

- apt-get

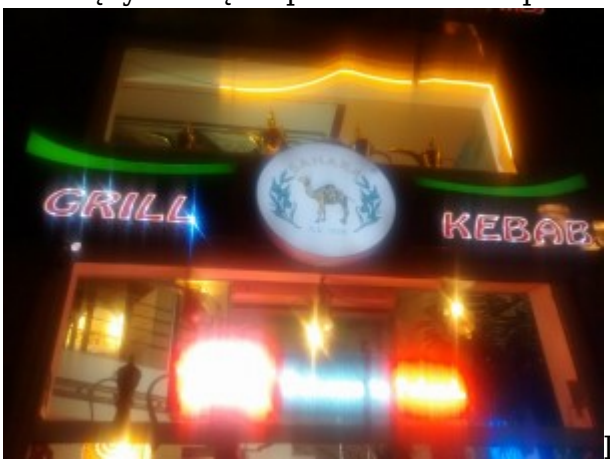
- boxnet
- dropbox
- ftp
- google-play
- ping
- skype
- skype-probe
- tor2web
- torch-browser
- traceroute
- yum
- bittorrent
- bittorrent-sync
- checkpoint-vpn
- ciscovpn
- cyberghost-vpn
- droidvpn
- gmail-drive
- kerio-vpn
- open-vpn
- packetix-vpn
- ssh-tunnel
- steganos-vpn
- tinyvpn
- tor
- vipnet-vpn
- wallcooler-vpn

Aplikacje, które się znalazły na liście znalazły się tam, ponieważ zostały uznane w danym momencie za zbędne użytkownikowi lub były zbyt uciążliwe/podejrzane.

Po ostatniej prelekcji pierwszego dnia na parterze PM, odbyło się małe afterparty. Cóż mogę napisać o afterparty? Nic. Tajemnica służbowa, kto nie był nigdy się nie dowie co stracił. Dzień skończył się „kalendarzowo” równo z 23:59:59 pierwszego dnia B-Sides.

Drugi dzień zaczął się od szybkiej pobudki, ogarnięcia i pośpiechu na tramwaj. Pomimo małej obsówki czasowej dotarliśmy na miejsce przed prelekcjami i zdążyliśmy uruchomić sieć na czas. Dzień ten minął bez większych wypadków technicznych, nie licząc jednego padu naszego AP. Niestety tego dnia, nie wszystkim dało się kulturalnie wytłumaczyć, dlaczego nie mogą używać swojego tajniackiego-hackierskiego Open-VPN'a na standardowym porcie. Koniec końców – była to jedyna osoba mająca odwagę podejść i zapytać o co chodzi. Poniekąd mogę się pochwalić sukcesem o którym pisałem już wcześniej. Każde zidentyfikowanie aplikacji, której nie ma opisanej w applipedi palo jest dla mnie sukcesem, tak samo było z wykryciem i zidentyfikowaniem „stunnel'u". Niezwykle ucieszyła mnie też prezentacja dwóch prawników – Jakuba Barańskiego i Krzysztofa Wojdyło. Gratuluję panowie wyjaśniliście dużo istotnych kwestii. Oczywiście, nie obędzie się i tym razem bez ślicznego obrazka. Ilustruje on jakie pliki pobierali użytkownicy drugiego dnia konferencji.

	Receive Time	File Name	Name	From Zone	To Zone	Source	Destination	To Port	Application	Action
	10/10 15:24:24	tcp_ip_illustrated_volume_1_the_protocols_2nd_edit.pdf	Adobe Portable Document Format (PDF)	internet	users	199.34.228.[redacted]	172.16.0.8	38032	web-browsing	alert
	10/10 15:24:02	tcp_ip_illustrated_volume_1_the_protocols_2nd_edit.pdf	Adobe Portable Document Format (PDF)	internet	users	199.34.228.[redacted]	172.16.0.8	59197	web-browsing	alert
	10/10 15:18:01	Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf	Adobe Portable Document Format (PDF)	internet	users	104.25.177.[redacted]	172.16.0.8	48914	web-browsing	alert
	10/10 15:15:56	tcpipb-2.pdf	Adobe Portable Document Format (PDF)	internet	users	188.117.147.[redacted]	172.16.0.8	41947	web-browsing	alert
	10/10 15:12:42	tcppr2.pdf	Adobe Portable Document Format (PDF)	internet	users	188.117.147.[redacted]	172.16.0.8	57325	web-browsing	alert
	10/10 14:13:59	EuroBSDCon2015-devsummit-IIJ-20151002-0.pdf	Adobe Portable Document Format (PDF)	internet	users	149.20.53.[redacted]	172.16.0.45	60739	web-browsing	alert
	10/10 14:04:28	F1299102015_NETpr.pdf	Adobe Portable Document Format (PDF)	internet	users	176.119.48.[redacted]	172.16.0.28	65437	web-browsing	alert
	10/10 13:44:02	blackarch.db	TAR	internet	users	38.229.66.[redacted]	172.16.0.37	36716	web-browsing	alert
	10/10 13:43:58	multilib-testing.db	TAR	internet	users	92.92.207.[redacted]	172.16.0.37	36948	web-browsing	alert
	10/10 13:43:38	extra.db	TAR	internet	users	92.92.207.[redacted]	172.16.0.37	36948	web-browsing	alert
	10/10 13:43:23	testing.db	TAR	internet	users	92.92.207.[redacted]	172.16.0.37	36948	web-browsing	alert
	10/10 10:21:08	098caf35-bfae-426a-b9e4-2f9db5063e28	Windows Executable (EXE)	internet	users	23.61.248.[redacted]	172.16.0.41	5508	web-browsing	alert

Mam nadzieję, że osoba patchująca sobie archa dzięki nam będzie bezpieczniejsza! Pod kątem abuse – spokojnie, można by rzec iż poza kilkoma dziwnymi ssh i zapytaniami webowymi kończącymi się odpowiedzi 401 spowodowanymi niedziałającym api to było spokojnie. 

Drugi dzień również zakończyliśmy afterparty. Myślę, iż istotną informacją jaką podam będzie fakt, że w carrefurze koło PM nie ma alkoholu – #sprawdzone info. Z PM powędrowaliśmy na klasyczne fast food adminów – kebab pod palmę. Jeśli ktoś tam nie jadł polecam serdecznie.

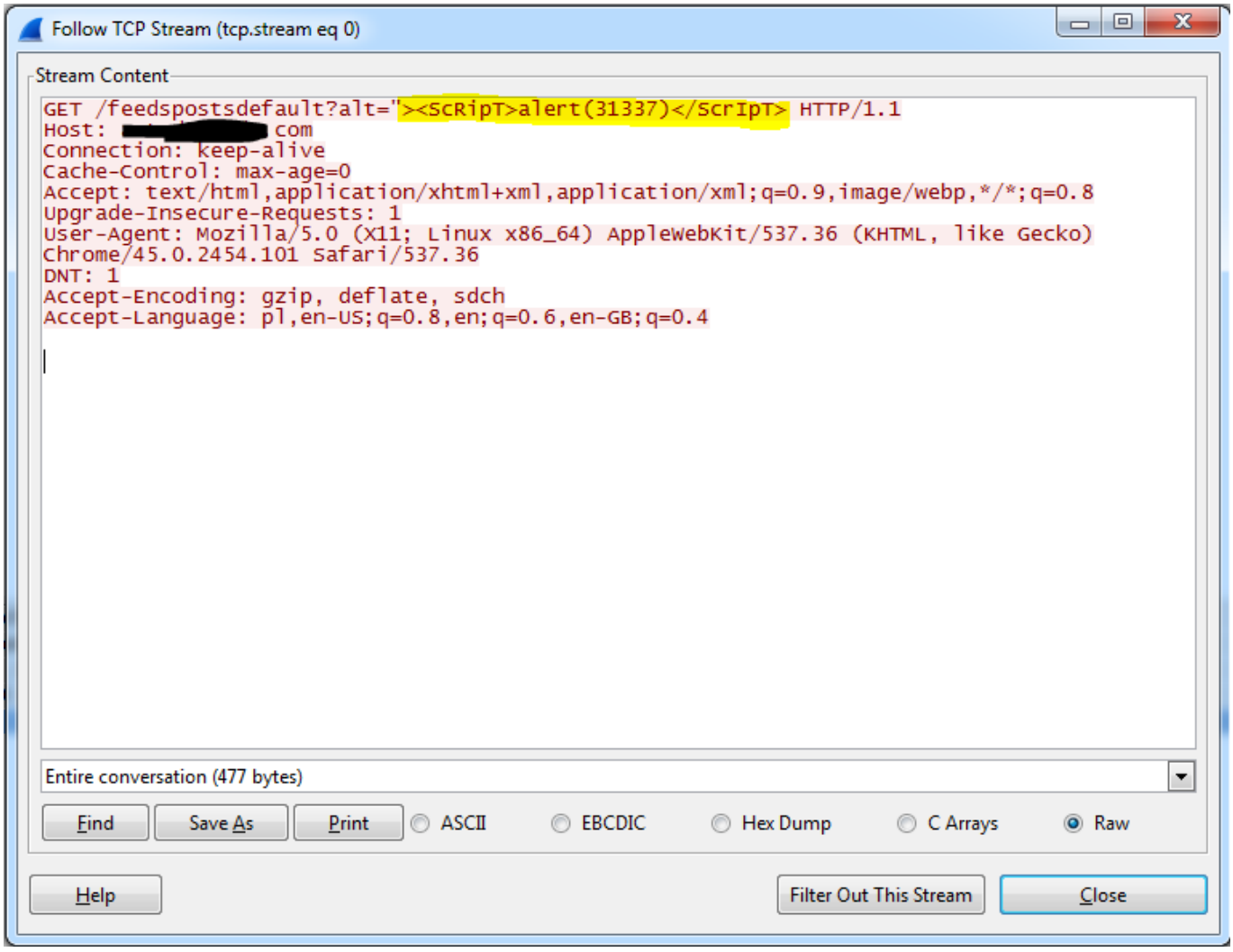
Po kebabie znów poszliśmy w okolice PM a dokładnie do Mekonga przy stacji metra Ratusz Arsenał. Jeżeli zaś, gdy będziecie w Warszawie, powie „Idziemy pod poniata” – na pewno nie ma na myśli podróży ZTM, a raczej Gandalfowe „Szukam kompanów do przygody”. Do domu udało mi się wrócić około 2-3 w nocy.

Trzeci dzień zaczął się małym fuckupem – tak, zaspałem, „budzik mi nie dzwonił” itd… – mimo to daliśmy rade dotrzeć na miejsce prawie idealnie na czas. Po szybkim uruchomieniu sieci, przygotowaniu transmisji przyszedł czas na moją prelekcję.

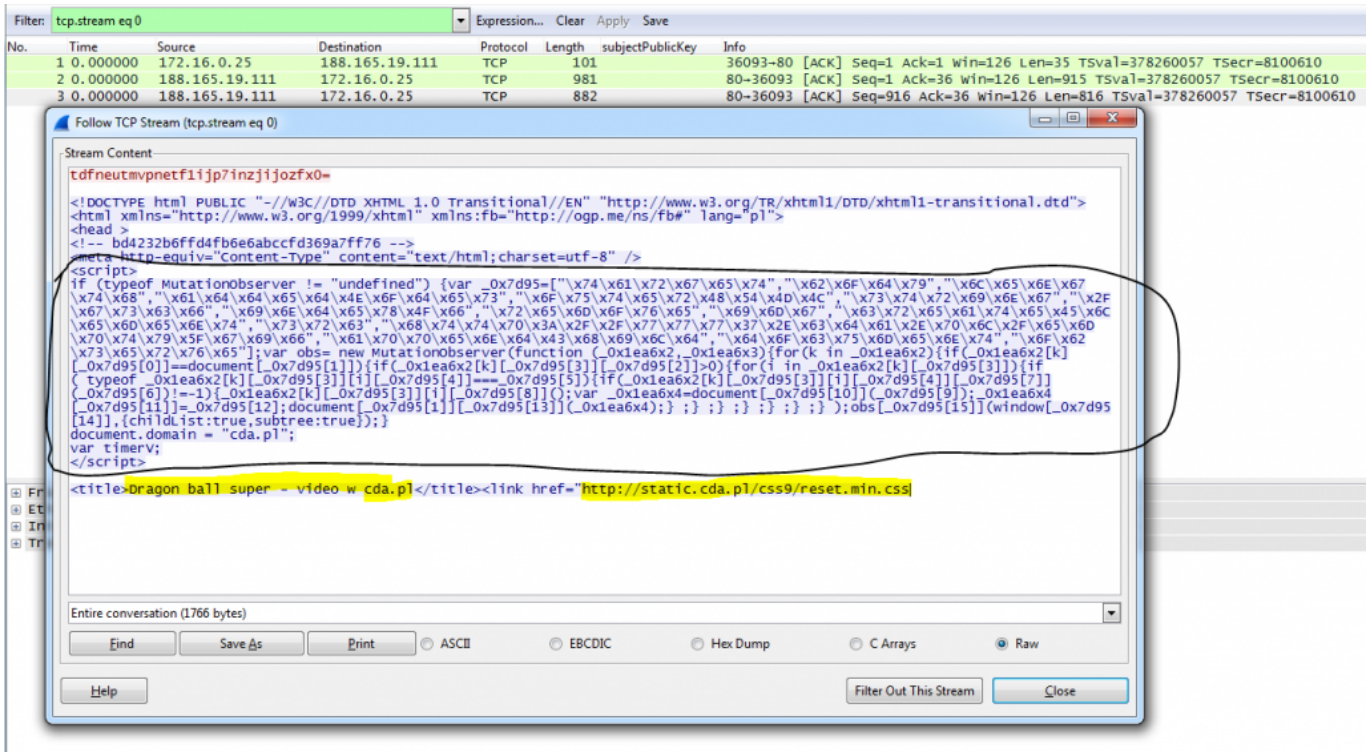
Kto nie oglądał na żywo lub wcześniej polecam serdecznie mu obejrzeć. Podczas swojego wystąpienia starałem się trochę przybliżyć moją wizję ideologii hackerstwa czy też po prostu powiedzieć jak ja widzę świat hakerów. Prezentację w formie pdf można pobrać tu.

Nie jestem zwolennikiem publicznego linczowania kogokolwiek, ale niestety trzeciego dnia doszło do sytuacji, która zmusiła mnie jako admina i nikowa jako organizatora do zdecydowanych kroków. Chodzi o sytuację, którą na pewno pamiętają osoby które były na sali podczas prezentacji Marcina Dudka. Zaraz po tej prelekcji wywołaliśmy jedną z osób na sali. Osoba ta początkowo nie reagowała na wezwania, potem twierdziła że nic nie zrobiła. W momencie w którym poinformowałem ową osobę o fakcie, iż sytuacja została zarejestrowana zaczęła się tłumaczyć, iż ataki były dokonywane na stronę/serwer należące do niej. Otóż nie.

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	Destination Country	To Port	Application	Action	Severity
		10/11 11:36:19	vulnerability	HTTP Cross Site Scripting Attempt	users	internet	172.16.0.13	216.239.32.[redacted]	US	80	web-browsing	reset-both	low
		10/11 11:36:15	vulnerability	HTTP Cross Site Scripting Attempt	users	internet	172.16.0.13	216.239.32.[redacted]	US	80	web-browsing	reset-both	low
		10/11 11:36:10	vulnerability	HTTP Cross Site Scripting Attempt	users	internet	172.16.0.13	216.239.32.[redacted]	US	80	web-browsing	reset-both	low
		10/11 11:36:10	vulnerability	HTTP Cross Site Scripting Attempt	users	internet	172.16.0.13	216.239.32.[redacted]	US	80	web-browsing	reset-both	low



Kolejną rzeczą, którą bedę opowiadał zapewne jako anegdotę to obfuskowany kod (nie sprawdzałem co robi dokładnie, ale brzydko wygląda) JavaScript na stronie… cda.pl. Myślę, że każdy zna cda.pl a jak ktoś nie zna, to za chwilę pozna. Cda.pl jest stroną zawierającą ogromną ilość filmów (tak tych które ogląda się za pieniążki na zalukaj.tv) udostępnia je darmowo, można tam znaleźć gry online… Taki tam polski youtube z grami.



Swoją drogą, będę musiał się kiedyś temu dokładnie przyjrzeć i przeanalizować co to dokładnie jest, może znajdzie się tam coś ciekawego.

Oczywiście, życzę również powodzenia osobą posiadającym podczas konferencji adresy ip: 172.16.0.7, 172.16.0.17, 172.16.0.25, 172.16.0.31, 172.16.0.45. Osoby te zostały całkowicie wycięte z sieci w względu na nagminne generowanie śmieciowego ruchu. Pozdrawiam również osobę, która poszukiwała odkurzacza bez workowego na allegro. Nie ukrywam, że trzeci dzień, chociaż najprzyjemniejszy (oczywiście najsmaczniejszy bo #karkówkanaobiad) miał też w sobie też trochę smutku który czuło się od rana. Przykra była myśl, że coś co było szykowane przez ostatnie kilka miesięcy, w co włożyło się tyle pracy właśnie się kończy. Ale nie można się smucić! Moje dzielne ptaszki doniosły mi, że być może już w kwietniu będzie możliwe jakieś psucie pod banderą SBS. Kiedy kolejny B-Sides? O to, pytajcie już orgów. Na koniec wspominek, mam dla was zdjęcie przedstawiające „siec.rar” czyli z czym wracaliśmy do pehatspejsu po konferencji.

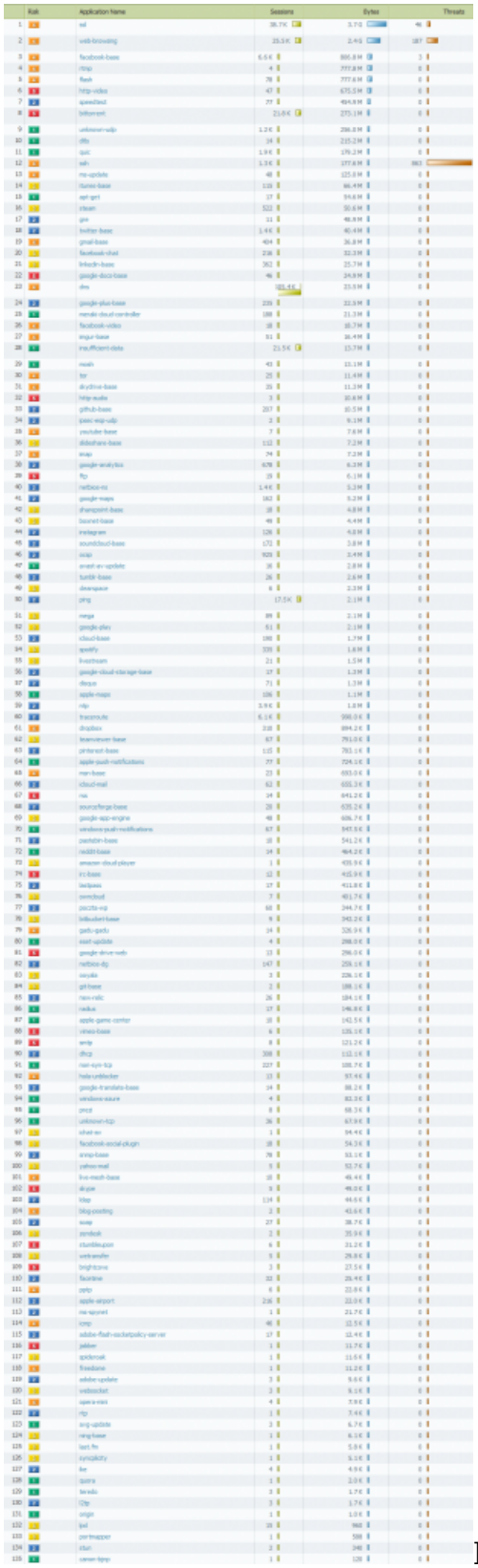
Na koniec podsumowania chcę przedstawić kilka dodatkowych obrazków przedstawiających jakie aplikacje czy kategorie url były popularne pośród użytkowników.

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	HIGH	SSH User Authentication Brute-force Attempt	40015	vulnerability	571
2	INFORMATIONAL	SSH2 Login Attempt	31914	vulnerability	292
3	INFORMATIONAL	HTTP Unauthorized Error	34556	vulnerability	160
4	LOW	SSLv3 Found in Server Response	36815	vulnerability	40
5	INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability	17
6	LOW	HTTP Cross Site Scripting Attempt	32658	vulnerability	4
7	LOW	JavaScript Obfuscation Detected	31825	vulnerability	2

Ilość incydentów bezpieczeństwa wykrytych przez palo.

	Category	Sessions	Bytes
1	not-resolved	19.5 K	2.5 G
2	computer-and-internet-info	6.6 K	1.3 G
3	content-delivery-networks	7.9 K	731.9 M
4	streaming-media	416	378.3 M
5	social-networking	4.5 K	346.4 M
6	online-storage-and-backup	309	252.7 M
7	search-engines	3.9 K	223.8 M
8	music	78	66.0 M
9	games	40	48.4 M
10	web-based-email	579	47.8 M
11	educational-institutions	160	34.3 M
12	web-advertisements	1.3 K	26.2 M
13	personal-sites-and-blogs	259	16.6 M
14	auctions	170	11.9 M
15	internet-portals	508	11.3 M
16	business-and-economy	243	8.7 M
17	news	289	8.4 M
18	reference-and-research	278	6.9 M
19	internet-communications-and-telephony	283	4.4 M
20	web-hosting	253	4.3 M
21	private-ip-addresses	139	3.6 M
22	shopping	92	2.6 M
23	parked	105	1.5 M
24	government	48	1.3 M
25	shareware-and-freeware	168	1.3 M
26	financial-services	60	525.5 K
27	translation	15	402.9 K
28	unknown	1	216.6 K
29	motor-vehicles	7	110.3 K
30	stock-advice-and-tools	3	28.8 K

Rozkład kategorii url'i które były popularne podczas konferencji. Segregacja względem ilości danych.



Pełna lista aplikacji webowych posegregowanych

względem ilości zutylizowanych danych. Przypominam, że każdą aplikacje z tej listy możecie sprawdzić tu. A teraz, do przeczytania!