Informe de resultados de actuación del appliance

Tipo de documento: Entregable
31/08/14

ecoRaee

Life

Universidad de Vigo

energylab

revertia

Tabla de contenidos del proceso demostrativo

Índice de tablas e ilustraciones

1.- Introducción

El objetivo de este demostrativo es la instalación y configuración de una máquina, con hardware basado en el reciclaje de ordenadores usados, que sirva de sistema de defensa perimetral para redes de PYMES y particulares. El uso de herramientas libres y preferentemente gratuitas propiciará una reducción de costes en la solución, frente a otros sistemas comerciales. Se persigue como objetivo esta reducción de costes para favorecer la entrada del producto en PYMES, que normalmente tienden a ser reacias a grandes inversiones tecnológicas, especialmente en el ámbito de la seguridad informática. El sistema será capaz de realizar las funciones de: antivirus, antispam, control de contenidos y firewall. Puede verse una definición de la arquitectura utilizada en la Ilustración 1.

Se han instalado diez appliances en distintas organizaciones, intentando abarcar el máximo de entornos diferentes en función de su naturaleza. Por ello, se han instalado appliances en empresas de fabricación de elementos mecánicos, empresas de servicios, empresas de desarrollo de software, centros educativos de enseñanza secundaria y centros educativos de enseñanza universitaria. De esta forma, se ha obtenido un espectro general de organizaciónes con un volumen importante de uso de internet dentro de sus funciones.

Para simplificar los resultados se han agrupado con una media de las instalaciones en empresas y las instalaciones en centros educativos para mejorar la evaluación de resultados.

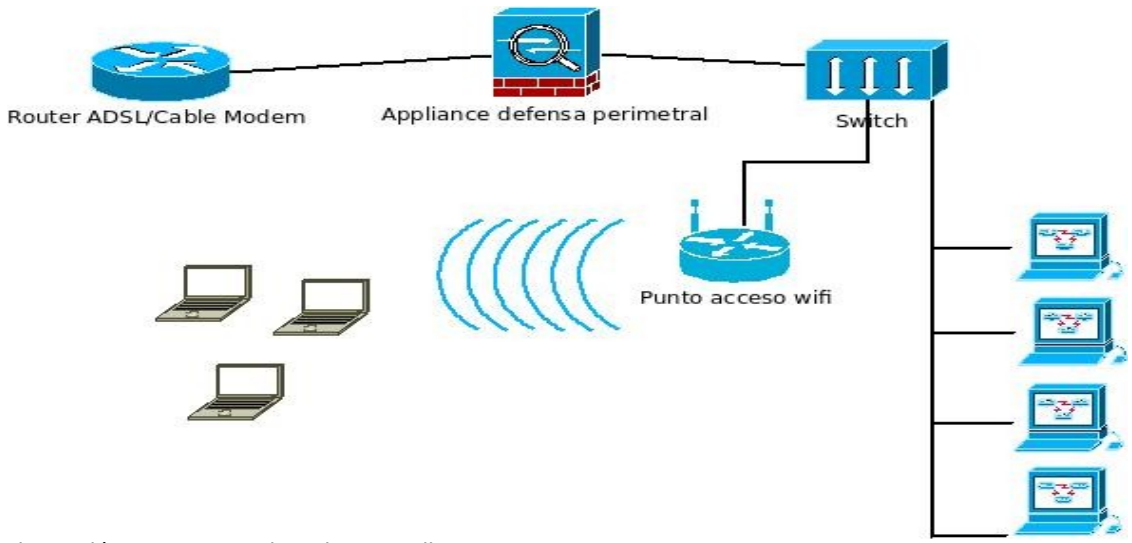


Ilustración 1: Esquema de red con appliance

2.- Resultados

Virus, información obtenida de los logs de HAVP

Tal y como se indicó en la introducción se establecen dos tipos de organizaciones para su estudio. Están marcados en los anexos como Enterprise y como Educational.

Mediante el siguiente comando btenemos el número total de ficheros vía tráfico web analizados, la rotación de ficheros de log se hace periódicamente, el tiempo total analizado fue de seis meses:

$ wc -l access.log*

Pueden verse los resultados en los anexo con el título VirusDataEnterprise y VirusDataEducational.

Nombres de los Virus, información obtenida de los logs de HAVP

Con la siguiente instrucción obtenemos el nombre de los virus encontrados, y el número de veces que aparece:

$ grep VIRUS * | awk 'BEGIN {FS="VIRUS"}{print $2}' | sed 's/ ClamAV: //g' | uniq -c

Hemos construido la gráfica de muestra de datos de manera que se manejen los porcentajes de aparición de cada virus en lugar de su ocurrencia. Pueden verse los resultados en los anexo con el título NameVirusEnterprise y NameVirusEducational.

Tráfico web, información obtenida de los logs de DansGuardian

Con esto obtenemos el número de elementos web analizados, cada elemento de cada web por separado, es decir en access.log por ejemplo no son 3431 páginas vistas, son elementos de webs: páginas, imágenes, frames externos …

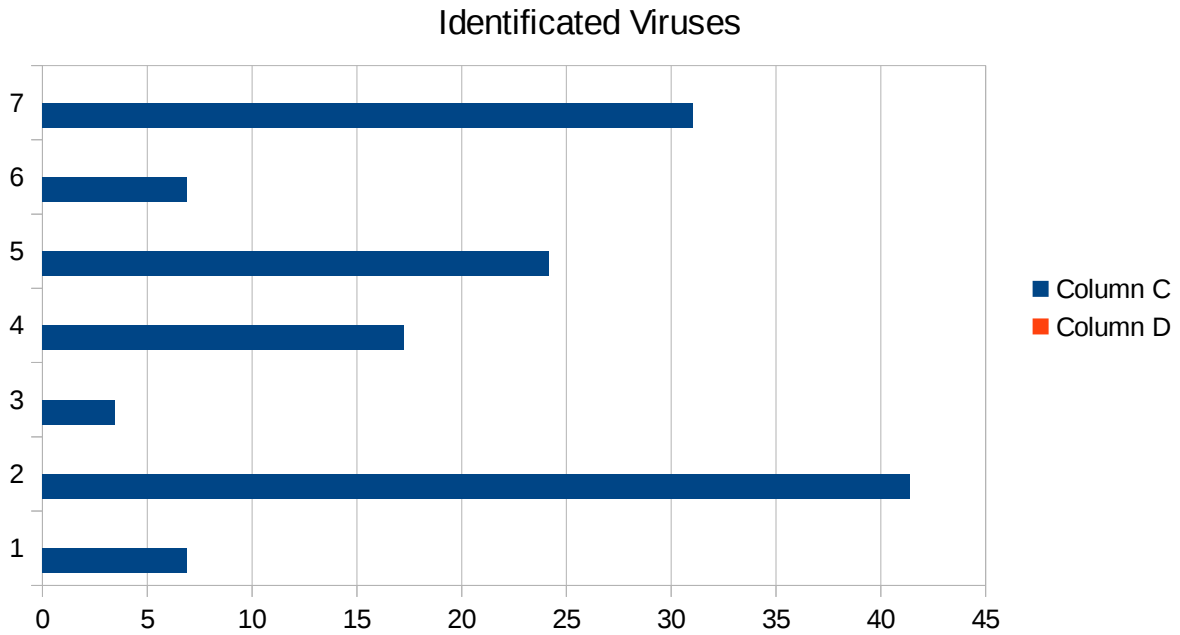
En este caso cada fichero de log es de un día pero en el análisis de resultado hemos realizado una agrupación por mes:

$ wc -l *

Pueden verse los resultados en los anexo con el título DansGuardianEnterprise y DansGuardianEducational.

3.- Anexos

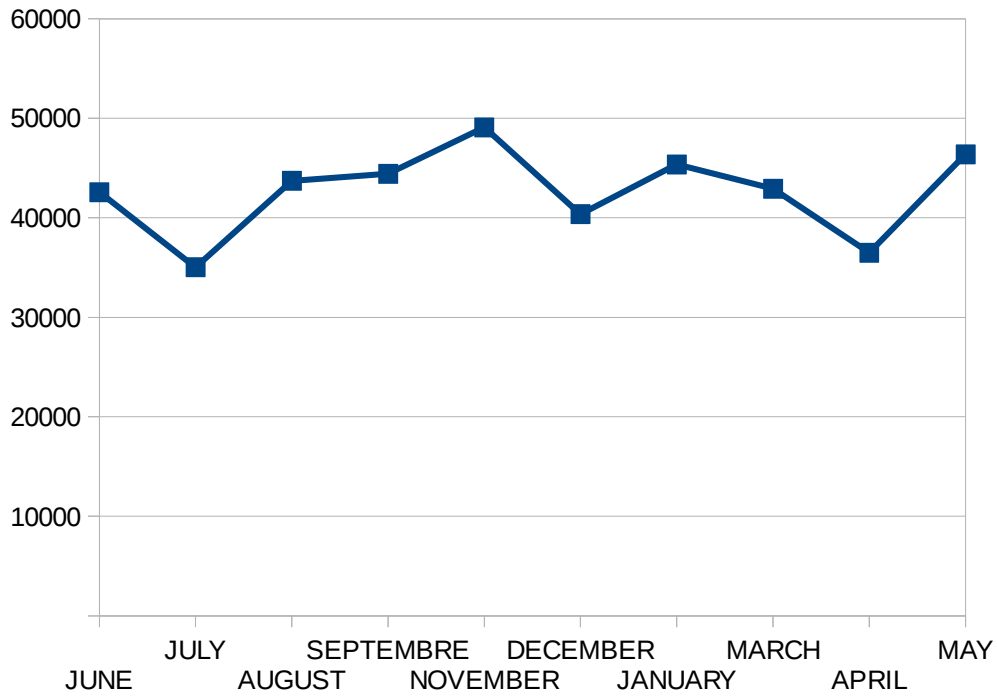
Porcent	Name
6,896551724	HTML.Exploit.CVE_2014_0322
41,37931034	Win.Adware.Toggle-4
3,448275862	Win.Trojan.11366268
17,24137931	Win.Adware.Outbrowse-2
24,13793103	Win.Adware.Agent-7725
6,896551724	Eicar-Test-Signature
31,03448276	Others



DansGuardian Enterprise

	JUNE	JULY	AUGUST	SEPTEMBRE	NOVEMBER	DECEMBER	JANUARY	MARCH	APRIL	MAY
1	1384	557	3336	659	748	1511	3368	884	2075	2874
2	1253	2744	1485	1830	890	68	727	3412	1078	1964
3	2249	1856	3125	2348	1716	2693	2560	732	2630	918
4	1188	1471	2294	2994	2054	1287	1432	1723	2309	1220
5	3274	31	686	1774	1400	2027	3339	2068	3245	626
6	2900	1162	3244	971	1115	981	103	642	2318	3144
7	503	1039	175	2057	3348	2540	1878	1632	1125	2884
8	725	118	2339	17	2643	15	2333	40	101	421
9	1670	544	2665	2560	793	350	825	302	184	1357
10	2157	3312	317	391	2546	2027	187	1669	1124	999
11	1464	1574	242	1916	3048	1159	1158	1519	1933	2633
12	720	437	2177	1715	96	986	440	2207	1622	1734
13	1676	1230	304	962	1330	3107	450	2781	351	451
14	2196	407	2844	2415	2842	409	1775	2262	374	2334
15	1214	3156	989	1751	2526	727	1687	1931	1577	3268
16	975	1637	652	3235	2184	1477	939	584	778	397
17	3261	1937	603	1444	344	588	2553	2551	1153	1886
18	3371	1184	1779	1498	2437	3159	2759	570	824	1712
19	2294	1077	2652	749	1113	394	3310	3271	2301	2565
20	44	2205	892	1540	225	2768	2119	1570	2991	2388
21	896	1998	2641	1638	2640	3249	3207	2842	2049	3075
22	771	529	1994	3352	2467	2440	3283	2186	1246	3256
23	3185	407	123	2953	1929	1832	99	2293	630	2653
24	2281	1786	301	1101	3127	615	1101	1101	289	1077
25	252	418	3334	1871	2725	636	2814	1314	692	72
26	669	2216	2527	690	2812	3329	919	843	1493	468
	42571	35032	43719	44431	49097	40373	45363	42928	36493	46378

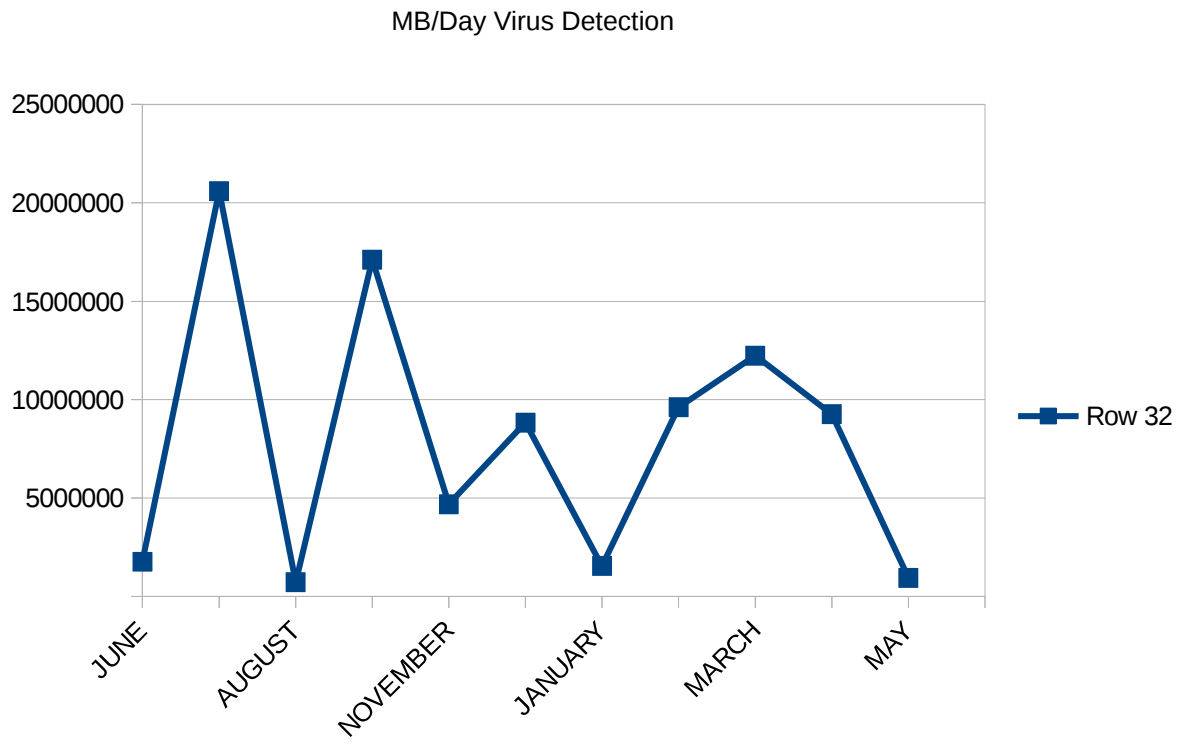
MB/Day of HTTP request



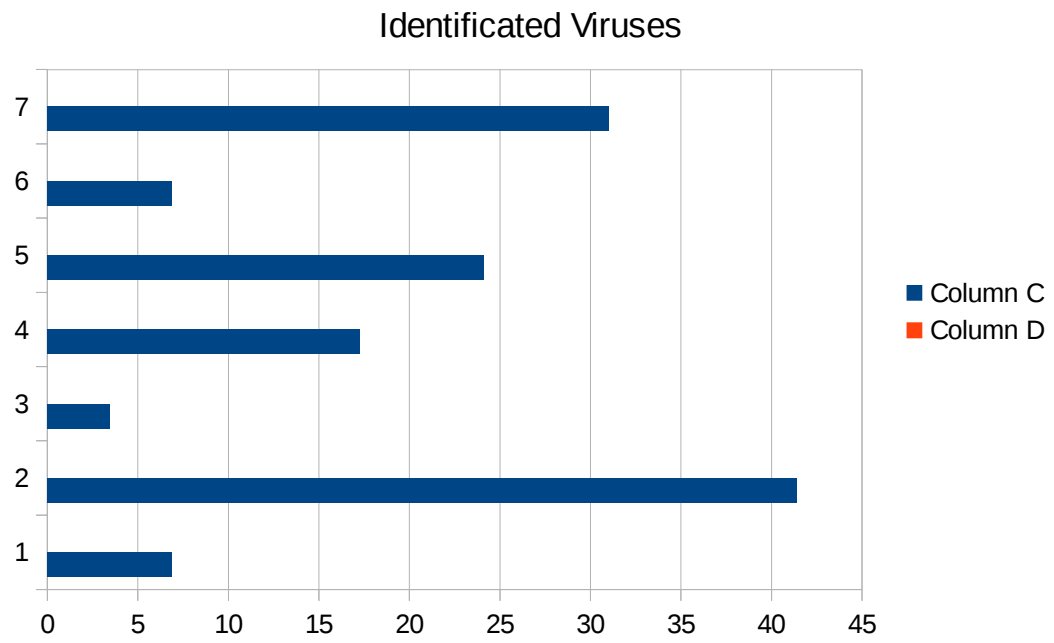
Virus Detection

	JUNE	JULY	AUGUST	SEPTEMBER	NOVEMBER	DECEMBER	JANUARY	FEBRUARY	MARCH	APRIL	MAY	
1	1289289	321465	720324	74911	720183	843194	743910	944028	941730	1170930	455338	
2	15684	252127	1	398557	53796	146400	9151	82164	586988	257463	41429	
3	11646	1378017		286341	299035	534308	5924	512329	608970	39981	477	
4	38251	699180		456116	13901	216853	47971	517900	377028	398026	48553	
5	2017	1071549		248224	153399	113976	46581	291531	21888	27685	3226	
6	2282	461534	1	499309	94677	144098	20321	648006	688108	453165	6606	
7	24066	1131359	1	323176	318195	241955	11076	578722	68316	152486	6074	
8	31846	806224	1	1047255	196822	89528	45154	137140	704607	375795	23530	
9	25133	370389		564110	6213	307013	69022	268954	97210	321495	12562	
10	29377	1010809	1	1086086	72499	661572	30526	586844	682242	479569	35694	
11	25719	503257	1	1125426	101301	538216	11833	160916	59020	172860	55028	
12	3765	590020		1006761	12407	395169	54142	372804	515336	115124	25812	
13	23982	710693		460881	308875	340757	61031	19158	691497	709274	35981	
14	32322	989676	1	1018878	296343	57031	51808	361249	232479	576003	3072	
15	41778	680549		1065910	311109	343820	37853	123325	29802	643895	9202	
16	12846	1218954	1	949451	151752	428706	20660	511067	653960	74698	14640	
17	17957	1291403	1	389350	335	207150	40900	470492	745772	39470	16026	
18	34784	815085		897006	224246	293153	26885	60712	487895	253215	10362	
19	785	1158648		726192	19028	367201	15224	352262	687400	167035	3451	
20	1189	1077584		472141	282784	685844	49276	185714	640395	21926	6636	
21	38230	265599	1	337720	204598	76757	2144	434685	528934	457562	30261	
22	15555	1007788		821416	258650	84175	56221	31010	287029	191190	31158	
23	18267	825507		875688	86331	385553	5384	575523	225852	377963	38137	
24	6323	274259		601502	131400	272407	9141	373435	584250	500494	5497	
25	5883	1017508		1258083	266682	416050	4446	570216	666078	743251	521	
26	13729	672019	1	126348	100176	639084	71344	448594	424351	542946	24391	
	1762706	20601203	720336	17116836	4684735	8829970	1547924	9618779	12237140	9263502	943662	

VirusDataEntreprise

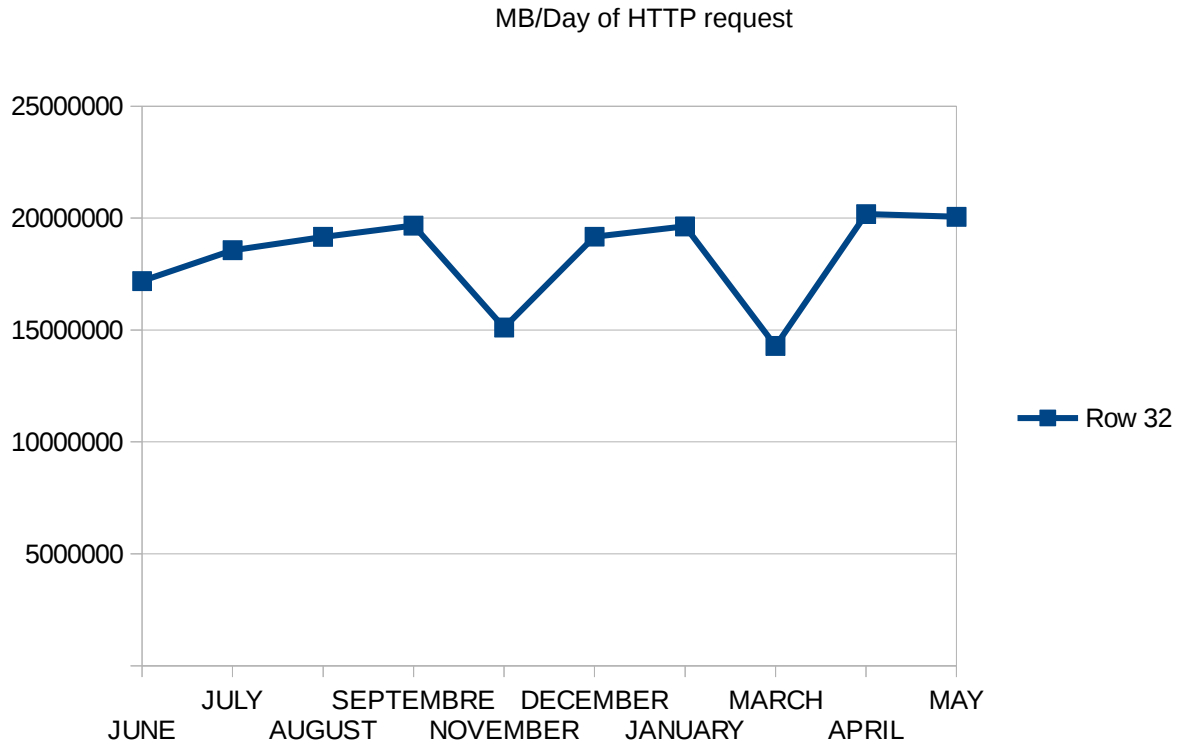


Porcent	Name
7,317073171	HTML.Exploit.CVE_2014_0322
21,95121951	Win.Adware.Toggle-4
7,317073171	Win.Trojan.11366268
17,07317073	Win.Adware.Outbrowse-2
21,95121951	Win.Adware.Agent-7725
7,317073171	Eicar-Test-Signature
17,07317073	Others

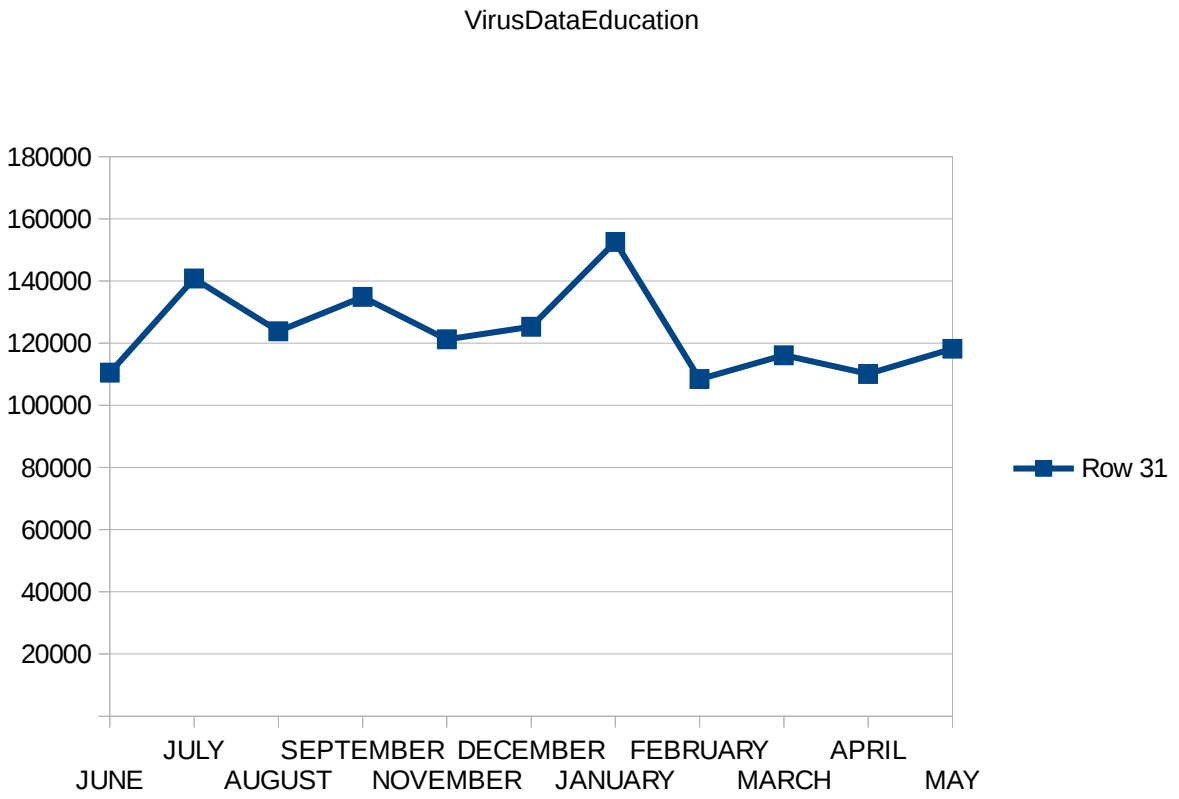


DansGuardian Education

	JUNE	JULY	AUGUST	SEPTEMBRE	NOVEMBER	DECEMBER	JANUARY	MARCH	APRIL	MAY
1	558741	568556	789859	19549	56350	683125	515048	906551	1169850	1307459
2	505685	627851	1322694	664345	585800	280105	1282387	654716	745286	1147460
3	908012	763614	294954	1305994	392642	664779	764682	498665	1317393	1239953
4	479612	177505	276335	934376	816694	995530	600017	319468	1089521	359404
5	1321829	549464	812713	1177094	876110	1296534	1040708	868610	1045622	337489
6	1170839	1102924	20444	1131653	1160721	950180	521068	38691	768943	1056576
7	202929	1193725	886393	514225	925586	1310460	557210	280503	817432	1136099
8	292522	771640	1094267	388742	189513	582915	838060	600495	594362	157766
9	674004	206008	260228	954227	392924	316854	1234495	463622	650246	74827
10	870796	1284575	729236	770358	480849	482619	136728	451484	766057	1375285
11	590971	178537	192284	568935	619289	612895	395794	623840	1025067	1078742
12	290495	794547	970519	1048828	941998	109835	771616	98026	303170	999982
13	676490	61840	1308376	368715	546317	504688	888780	1030142	880204	707529
14	886434	987407	384945	1035890	120508	670965	665206	166752	1319663	1023302
15	490056	981954	1271211	746879	454470	571087	669090	1256649	233663	575348
16	393705	654150	334955	367076	979154	943674	639425	861271	590414	573170
17	1316352	46888	949363	1075638	544389	1365156	821489	296061	81403	672732
18	1360710	1321430	397253	1227256	372102	710871	1003121	84875	812195	506986
19	925879	1034837	737049	475653	318255	121194	1182910	587722	581614	682589
20	17825	984644	890629	135564	1190262	69033	80158	935253	945028	581417
21	361775	231281	243747	1188529	931444	883261	598386	316412	630573	1104254
22	311399	1272884	588277	778868	83440	1200317	1360808	265789	432321	575641
23	1285854	957611	1081944	77502	352428	1136540	1122891	538006	1160233	728747
24	920975	845800	774663	758799	175926	861804	972691	871621	1005201	163681
25	101655	288178	1313468	1161865	264595	1093775	74880	200155	39588	1054007
26	269927	676149	1237355	788966	1336377	751127	891009	1074005	1175689	835320
	17185472	18563998	19163161	19665525	15108145	19169322	19628658	14289384	20180736	20055764


MB/Day of HTTP request
25000000
20000000
15000000
10000000
5000000
JUNE
JULY
AUGUST
SEPTEMBRE
NOVEMBER
DECEMBER
JANUARY
MARCH
APRIL
MAY
Row 32

	JUNE	JULY	AUGUST	SEPTEMBER	NOVEMBER	DECEMBER	JANUARY	FEBRUARY	MARCH	APRIL	MAY	
1	1733	14728	5174	3513	14044	11410	11095	4830	2567	13431	6091	
2	18520	12151	848	9075	17737	11496	13841	6338	15049	9999	10549	
3	5583	4938	2860	489	238	2384	2507	1204	4727	3438	3705	
4	4338	3475	8841	9737	9802	3692	4577	3430	4693	2678	381	
5	217	387	597	581	137	83	470	219	251	83	318	
6	12954	7177	12296	11742	7713	4595	11394	8573	3053	5819	9419	
7	1641	165	1218	1199	1519	1272	572	581	1770	1011	501	
8	606	1453	853	934	188	865	1446	1833	188	308	138	
9	895	3146	1454	1218	2161	2308	2527	2205	67	767	1399	
10	7671	14002	10225	11328	8817	3049	11939	2540	3218	4021	10390	
11	1287	3018	642	3795	4796	2098	1449	604	3579	2408	3301	
12	6889	6134	7006	4474	5321	8423	6214	3701	7518	6867	3066	
13	91	2779	4328	5706	1365	1875	5305	3111	2799	4961	3488	
14	578	8858	12940	12695	8526	6332	14331	7781	6187	8643	6256	
15	2625	1322	2950	953	633	198	3462	1967	1029	2927	3759	
16	1708	9009	369	10567	1809	12852	4340	13935	3063	13601	7456	
17	7121	2690	6912	2109	9939	10160	6362	12481	1326	6062	1490	
18	417	283	8772	9712	1068	8762	6975	165	10111	4400	8782	
19	5761	176	2107	2226	291	1020	3588	1122	5036	2070	3759	
20	776	5399	4869	5485	69	1895	3408	238	5192	2601	6800	
21	13174	13571	6541	8196	10144	2639	1706	14015	16165	3419	984	
22	3365	12016	6708	6667	7412	9682	9098	2776	9692	6440	10561	
23	4754	7269	8495	4862	3026	1211	8792	8862	5277	2346	7044	
24	2618	29	920	638	618	1055	1201	1577	988	750	2223	
25	5015	6532	5748	6791	3553	15664	15979	4143	2415	815	6142	
26	161	109	185	211	320	301	24	227	153	268	203	
	110499	140817	123859	134904	121247	125321	152602	108458	116115	110131	118206	


VirusDataEducation
180000
160000
140000
120000
100000
80000
60000
40000
20000
JUNE
JULY
AUGUST
SEPTEMBER
NOVEMBER
DECEMBER
JANUARY
FEBRUARY
MARCH
APRIL
MAY
Row 31