HostExploit

World Hosts Report

Сентябрь 2013

Краткое содержание

Впервые хостинг-провайдеры, зарегистрированные в одной стране (США), заняли 3 лидирующих позиции в Top 50 рейтинга Хостов и Сетей.

На сегодняшний день как никогда актуальным является анализ существующих сервисов и стандартов хостинг-провайдеров с целью поиска необходимых усовершенствований существующей системы, которая имеет несколько вынужденных ограничений.

Количественное измерение уровня активности киберпреступности на серверах по всему миру является одним из способов достижения данной цели. С 2009 года компанией HostExploit исследовано более 43 000 публичных маршрутизируемых Автономных Систем по всему миру, собрано данные об инфицированных сайтах, ботнетах, а также проявлениях спама и аналогичной вредоносной активности. Полученные данные сводятся и анализируются доверенными источниками сообщества, а затем публикуются в рамках в рамках World Hosts Report (ранее – Топ-50 Наиболее Опасных Хостингов).

Данное исследование рекомендуется для ознакомления провайдерам интернет-услуг, специалистам по информационной безопасности, вебмастерам, а также руководителям технических разделов. В целом читателю предоставляется возможность сделать собственные выводы, так как цифры говорят сами за себя. Однако стоит подчеркнуть, что преобладающая часть вредоносного контента размещается в сети не сознательно. Зачастую это происходит в результате бездействия, а иногда хостинг компании попросту становятся жертвами.

Тем не менее, абсолютно достоверным остается тот факт, что инструменты для кибер-атак и все «зло» интернета где-то и кем-то размещено и при этом имеет свой #AS. Поэтому именно отсюда имеет смысл начать поиски решения существующей проблемы.

- Джарт Армин

ISBN 978-0-9836249-6-7

Сравнительные данные

AA419

Abuse.CH

Clean-MX.DE

Cyscon SIRT

Emerging Threats

Google Safe Browsing

Group-IB

HostExploit

hpHosts

ISC

KnujOn

MalwareDomains

MalwareDomainList

RashBL

Robtex

Shadowserver

SiteVet

Spamhaus

SRI International

StopBadware

SudoSecure

Team Cymru

The Measurement Factory

UCE-Protect

Редактор

Jart Armin

Рецензенты

Dr. Bob Bruen

Raoul Chiesa

Peter Kruse

Andre' DiMino

Thorsten Kraft

Andrey Komarov

Godert Jan van Manen

Steven Dondorp

Edgardo Montes de Oca

Авторы

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

Совместно с ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

NORTHWAVE

cyscon

SITEVET

montimage

Партнер проекта ACDC

ACDC
the Advanced Cyber Defence Centre

Оставайтесь на связи

Если наша деятельность близка Вам по духу, и Вы хотели бы принять в ней участие, тогда почему бы Вам не стать нашим спонсором или партнером?

Мы постоянно ищем возможности улучшить нашу деятельность путем расширения ее масштабов.

Если Вы считаете, что можете быть нам полезны, мы с радостью выслушаем Ваши предложения.

Пишите нам по адресу:

contact@hostexploit.com

Колонка редактора

Впервые хостинг-провайдеры, зарегистрированные в одной стране (США), заняли 3 лидирующих позиции в Top 50 рейтинга Хостов и Сетей.

Top 3 составили: AS33182 HostDime.com, AS26347 DreamHost, и AS11042 Landis Holdings. В рамках исследования, охватывающего три месяца второго квартала 2013 года, данные компании были классифицированы как хостинг-провайдеры с наивысшей концентрацией вредоносной активности, включая вредоносное ПО, спам-активность и ботнеты

Данный рекорд, разумеется, не является поводом для гордости. На протяжении длительного периода времени, авторитетные источники предупреждали о высоком уровне вредоносной активности в США, в частности, связанной с фишингом[1,2].

Что же послужило причиной этому? Основные факторы:

- Большое количество хостинг-провайдеров и низкие цены.
- Высокая интегрированность с сервисами анонимизации. Большинство регистраторов доменов и хостингов-провайдеров предлагают услугу 'whois proxy' и расширенные возможности оплаты через Bitcoin.
- Хорошая репутация. Минимальные шансы блокировки по критерию страны и повышенное доверие к веб-сайтам – идеальная среда для фишинг-проектов.

Однако для Соединенных Штатов есть и хорошие новости. В рейтинге стран они демонстрируют позитивные тенденции и опускаются с 5 места на 9. Поспособствовали улучшению позиции исключительно хорошие индивидуальные показатели нескольких хостинг-провайдеров (в том числе AS21740 eNom – 1150 номер рейтинга, и AS33626 Oversee – 943 номер рейтинга), в прошлом занимающих высокие позиции.

Итак, главная хорошая новость: хосты все-таки можно очистить. Но какие для этого нужны стимулы?

В настоящий момент на законодательном уровне таких стимулов очень мало. Международные действия очень сложны, а права потребителя отличаются от страны к стране, если вообще существуют. К примеру, в США провайдеры противостоят попыткам Федеральной комиссии связи ввести промышленные стандарты и отчетность, что сделало бы возможным штрафные санкции за недостаточную защиту потребителя.

Но даже при отсутствии денежных штрафов хостинг-провайдерам выгодно придерживаться «хороших практик» и прилагать все возможные усилия для поддержания своей чистоты. Это дает разнообразные преимущества – так будет лучше для бизнеса, экономики и национальной безопасности.

1 http://www.zdnet.com/blog/security/how-many-people-fall-victim-to-phishing-attacks/5084

2 http://www.gartner.com/newsroom/id/936913

Методология

В декабре 2009 года мы создали «Индекс HE», являющийся количественным показателем «вредоносности» Автономной Системы (AS). Несмотря на то, что в целом он был хорошо принят сообществом, с тех пор мы получили много конструктивных вопросов. На некоторые из них мы попытаемся ответить далее.

Почему в списке вместо абсолютной вредоносности представлена относительная?

Ключевая характеристика индекса делится на размер адресного пространства, выделенного конкретной AS, и поэтому она не представляет информации о суммарной вредоносной активности, ведущейся с этой AC. Статистика по сумме вредоносной активности, несомненно, была бы полезна вебмастерам и системным администраторам, желающим ограничить маршрутизируемый трафик, но все же целью Индекса HE является отражение уровня халатности мировых хостинг-провайдеров, важную роль в которой играют вольная трактовка и нарушения законодательства.

Разве большие организации не должны быть ответственны за реинвестирование прибыли в обеспечение безопасности?

Индекс HE придает больший вес AC с меньшим адресным пространством, но это отношение не линейно. Мы использовали "фактор неуверенности", или Байесовский фактор, для моделирования этой ответственности, благодаря чему для больших адресных пространств получены большие цифры. Чтобы усилить этот эффект, в этом отчете пороговое адресное пространство было увеличено с 10,000 до 20,000.

Если эти цифры не предназначены для вебмастеров, то для кого же они?

Чтение этого отчета рекомендуется вебмастерам – это позволит им получить жизненно важное понимание того, что происходит в мире информационной безопасности за пределами их ежедневных обязанностей. Тем не менее, наша главная цель – это повышение сознательности в вопросе главной причины всех проблем с безопасностью. Индекс HE является числовым представлением того, насколько в разных организациях разрешена незаконная активность – а точнее, насколько им не удается ее предотвратить.

Почему хостинг-провайдеры позволяют такого рода активность?

Важно отметить, что, публикуя данные результаты, HostExploit не утверждает, что перечисленные хостинг-провайдеры сознательно дали согласие на осуществление незаконной деятельности на своих серверах. Важно помнить о том, что многие хостинг-провайдеры также являются жертвами киберпреступности.

Ограничение ответственности

Были предприняты все возможные усилия, чтобы собрать для данного исследования максимально свежие, точные и полные данные, доступные на момент проведения анализа. Однако мы не заявляем, что данное исследование не содержит ошибок. Данные, которые были использованы, могут подвергаться обновлению и исправлению без предварительного уведомления.

Компания HostExploit, или какой-либо из ее партнеров, включая CyberDefcon, Group-IB и CSIS, не несет ответственности за неправильно поданные, неверно истолкованные или каким-либо образом измененные данные. Произвольные выводы и анализ, сделанный на основе таких данных, не может считаться результатом работы компании HostExploit или кого-либо из наших партнеров.

Определения

IP-адреса

В настоящем исследовании термин "IP-адреса" обозначает количество первичных IPv4-адресов, выделенных конкретной Автономной Системе (AS). Когда речь идет о странах, "IP-адреса" обозначают общую сумму IP-адресов всех Автономных Систем страны.

Страна

Поскольку Автономные Системы обычно физически маршрутизируют через несколько стран, HostExploit определяет наиболее вероятную страну происхождения Автономной Системы исходя из ее месторасположения и данных о регистрации.

Индекс HE

Количественный показатель HostExploit, представляющий концентрацию вредоносной активности, исходящей из данной Автономной Системы.

Рейтинг

Положение Индекса HE в рейтинге 44,556 Автономных Систем.

Более подробная информация содержится в разделе «Глоссарий».

Top 50 Хостов

Список 50 Автономных Систем с самыми высокими Индексами HE, т.е. с самой высокой концентрацией вредоносной активности.

Автономная система (AS)

Логическая совокупность Интернет маршрутов, контролируемых одной организацией или провайдером интернет-услуг.

#AS

Уникальный порядковый номер AC.

Индекс HE

Количественный показатель HostExploit, представляющий концентрацию вредоносной активности, исходящий из конкретной Автономной Системы.

Рейтинг

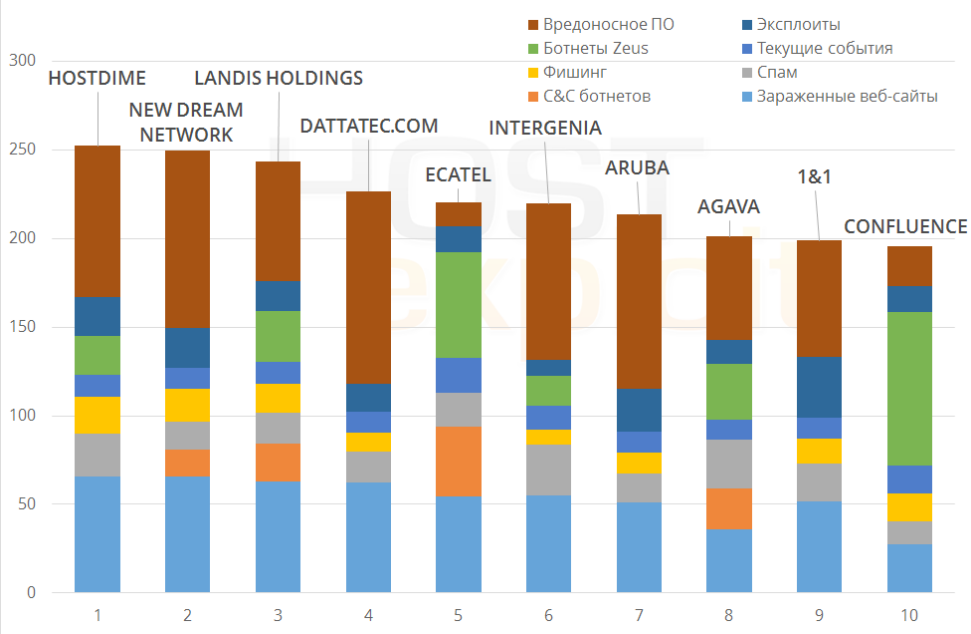
Положение Индекса HE в рейтинге 44,556 Автономных Систем.

IP-адреса

Количество IP-адресов, выделенных конкретной AC.

Рейтинг	Индекс	#AS	Название	Страна	IPs
1	252.33	33182	HostDime.com, Inc.	US	63,232
2	249.28	26347	New Dream Network, LLC	US	230,656
3	243.51	11042	Landis Holdings Inc	US	28,416
4	226.75	27823	Dattatec.com	AR	8,192
5	220.57	29073	Ecatel Network	NL	13,312
6	219.59	8972	Intergenia AG	DE	149,760
7	213.56	31034	Aruba S.p.A.	IT	145,664
8	201.20	43146	Agava Ltd.	RU	19,712
9	198.72	8560	1&1 Internet AG	DE	370,176
10	195.66	40034	Confluence Networks Inc	VG	12,288
11	194.54	47583	Hostinger International	US	11,008
12	193.03	25532	Masterhost	RU	77,824
13	191.61	12824	home.pl	PL	204,800
14	184.51	34619	Cizgi Telekomunikasyon	TR	30,208
15	183.00	29182	ISPsystem	RU	44,288
16	178.01	30633	Leaseweb USA	US	14,592
17	174.69	46606	Unified Layer	US	508,416
18	162.44	26496	GoDaddy.com, LLC	US	1,636,352
19	162.05	39743	Voxility S.R.L.	RO	55,808
20	156.79	16276	OVH Systems	FR	1,170,944
21	154.97	44112	SpaceWeb JSC	RU	3,584
22	154.50	50465	IQHost Ltd	RU	2,048
23	150.71	48159	Telecommunication Infrastructure	IR	192,256
24	150.55	16265	LeaseWeb B.V.	NL	365,312
25	149.34	51559	Netinternet	TR	18,432
26	148.55	36351	SoftLayer Technologies Inc.	US	1,401,344
27	141.61	25504	Vautron Rechenzentrum AG	DE	22,784
28	138.73	42612	ASN de Dinahosting SL	ES	18,432
29	137.64	24940	Hetzner Online AG	DE	639,744
30	137.20	4134	Chinanet Backbone	CN	116,932,576
31	132.51	46475	Limestone Networks, Inc.	US	90,112
32	131.42	15626	ITL Company	UA	19,200
33	130.18	41126	JSC Centrohost	RU	4,096
34	130.16	38731	Vietel - CHT Compamy Ltd	VN	28,672
35	126.28	58001	Ideal Solution Ltd	RU	2,560
36	125.61	32475	SingleHop	US	419,584
37	124.85	42244	eServer.ru Ltd.	RU	33,536
38	124.45	57668	Santrex Internet Services	SC	5,632
39	122.56	6147	Telefonica del Peru	PE	2,048,768
40	121.23	21844	ThePlanet.com Internet Services	US	1,509,376
41	120.63	8358	GTS Hungary	HU	30,720
42	120.21	15169	Google Inc.	US	669,696
43	118.32	47869	Netrouting Data Facilities	NL	23,040
44	118.27	9891	CS Loxinfo	TH	23,296
45	118.07	21219	Datagroup	UA	140,544
46	117.55	31815	Media Temple, Inc.	US	113,152
47	116.79	48031	PE Ivanov Vitaliy Sergeevich	UA	15,616
48	116.60	29550	Simply Transit Ltd	GB	116,224
49	115.81	18479	Universo Online S.A.	BR	24,064
50	115.49	41079	SuperHost.pl	PL	4,864

Top 10 Visual Breakdown



Что это?

Диаграмма слева дает визуальное представление о том, как каждый сектор активностей влияет на значение индекса АС.

Она позволяет наглядно увидеть, в каком направлении хостингу необходимо проводить улучшения в первую очередь.

Top 10 Новичков

Нижеследующие 10 АС имеют наиболее высокий рейтинг среди всех 2,058 АС, зарегистрированных с момента публикации последней версии исследования. Данная информация может представлять интерес в будущем.

Рейтинг	Индекс НЕ	#AS	Название	Страна	IPs
60	110.1	132524	Tata Institute	IN	512
193	74.1	12860	Axarnet Comunicaciones SL	ES	6,912
464	51.7	60751	Joshua Jameson / ServeByte	IE	1,024
484	50.7	43449	Dimline Ltd.	RU	512
613	45.1	55293	A2 Hosting, Inc.	US	24,576
923	34.5	35042	ISP4P IT Services	DE	26,624
937	34.2	199094	Accord OOD	BG	1,536
1,015	31.7	61036	JSC Dadeh Pardazi Fanava	IR	41,984
1,064	30.6	132497	Smartlink Broadband Services	IN	9,984
1,636	22.2	132527	Department of Posts	IN	1,024

Количество АС

В отчете за март 2013 года
43,454

В данном отчете
44,556

Новых АС
2,058

Удалено АС
956

Общее количество увеличено на
1,102

Что это?

Мы рассчитываем индекс каждой страны, используя метод аналогичный тому, который используется для расчета индекса отдельно взятой АС.

Индекс страны учитывается, если уровень вредоносной активности превышает порог в 1,000 пунктов; рассчитывается без привязки к количеству хостов в стране.

Таблица справа демонстрирует Top 10 стран, индексы которых были рассчитанных с помощью данного метода, а также 3 сектора активностей, которые имеют наиболее высокие индексы.

Top 10 Стран

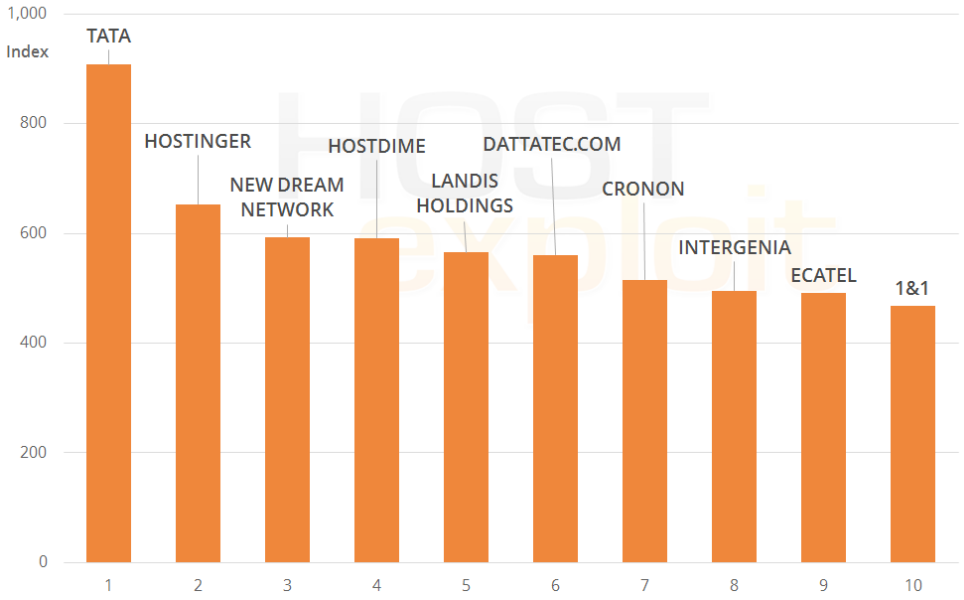
Страна	Название	ASes	IPs	Рейтинг	Индекс
VG	VIRGIN ISLANDS, BRITISH	6	18,688	1	435.5
	Highest sector		Infected web sites	1	905.3
	2nd-highest sector		Botnet C&Cs	1	889.0
	3rd-highest sector		Current events	1	823.9
PL	POLAND	1,590	21,932,032	3	306.7
	Highest sector		Current events	3	666.7
	2nd-highest sector		Phishing	2	648.1
	3rd-highest sector		Zeus botnets	4	431.7
RU	RUSSIAN FEDERATION	4,095	55,361,280	7	249.8
	Highest sector		Badware	3	502.5
	2nd-highest sector		Phishing	7	488.2
	3rd-highest sector		Current events	7	386.9
HU	HUNGARY	173	5,100,544	4	276.9
	Highest sector		Phishing	1	909.0
	2nd-highest sector		Current events	2	718.4
	3rd-highest sector		Zeus botnets	3	437.5
DE	GERMANY	1,294	119,035,296	6	251.3
	Highest sector		Zeus botnets	2	478.0
	2nd-highest sector		Current events	6	390.7
	3rd-highest sector		Phishing	11	261.1
KG	KYRGYZSTAN	27	300,544	8	242.9
	Highest sector		Badware	2	861.2
	2nd-highest sector		Exploit servers	2	465.7
	3rd-highest sector		Infected web sites	6	273.7
TR	TURKEY	304	21,711,872	10	238.7
	Highest sector		Current events	4	508.8
	2nd-highest sector		Zeus botnets	7	326.6
	3rd-highest sector		Botnet C&Cs	8	237.5
SC	SEYCHELLES	7	84,992	18	162.0
	Highest sector		Exploit servers	1	905.5
	2nd-highest sector		Infected web sites	2	840.8
	3rd-highest sector		Current events	171	68.4
US	UNITED STATES	14,573	1,233,079,112	12	218.1
	Highest sector		Current events	11	302.4
	2nd-highest sector		Zeus botnets	10	257.1
	3rd-highest sector		Phishing	13	241.0
UA	UKRAINE	1,666	15,120,384	11	221.1
	Highest sector		Badware	4	394.9
	2nd-highest sector		Phishing	9	284.2
	3rd-highest sector		Current events	13	283.3

Зараженные веб-сайты

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
907.2	132524	Tata Institute	IN	512	60	110.1
653.1	47583	Hostinger International	US	11,008	11	194.5
592.0	26347	New Dream Network, LLC	US	230,656	2	249.3
591.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
564.9	11042	Landis Holdings Inc	US	28,416	3	243.5
560.5	27823	Dattatec.com	AR	8,192	4	226.8
515.1	25504	Vautron Rechenzentrum AG	DE	22,784	27	141.6
495.5	8972	Intergenia AG	DE	149,760	6	219.6
490.6	29073	Ecatel Network	NL	13,312	5	220.6
467.3	8560	1&1 Internet AG	DE	370,176	9	198.7

Все три верхние позиции суммарного Индекса НЕ занимают высокую позицию в этой категории: AS26347 DreamHost – №3, AS33182 HostDime – №4, и AS11042 Landis – №5.

№1 в данной категории – AS132524 Tata – недавно зарегистрирован в Индии и имеет небольшое число IP-адресов. Именно с этим можно связать тот факт, что данный хост используется для предоставления временных услуг, или в качестве “одноразового ASN”.



Знаете ли Вы?

В данный рейтинг входят все хостинг-провайдеры, попавшие в Top 7.

Статистика

AS132524 Tata находится на 8-м месте по количеству инфицированных веб-сайтов в Топ 10, однако тот факт, что он является довольно небольшой единицей, ставит его на первое место.

Знаете ли Вы?

Sotal-Interactive и ISPsystem преимущественно распространены в России, но зарегистрированы в Украине и Люксембурге, соответственно.

C&C ботнетов

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
1,000.0	50465	IQHost Ltd	RU	2,048	22	154.5
488.4	61322	Sotal-Interactive ZAO	RU	256	414	55.2
475.7	56617	SIA "VPS Hosting"	LV	1,024	168	76.4
474.4	29182	ISPsystem	RU	44,288	15	183.0
415.0	26230	Telecom Ottawa Limited	CA	21,504	586	46.6
404.8	46785	Quasar Data Center, Ltd.	US	6,656	236	67.6
351.9	29073	Ecatel Network	NL	13,312	5	220.6
318.9	29141	Bradler & Krantz GmbH	DE	19,456	55	113.4
294.3	47900	Art-master LLC	UA	256	950	33.7
292.1	47161	KosmoHost IT Technologies	RU	512	966	33.4

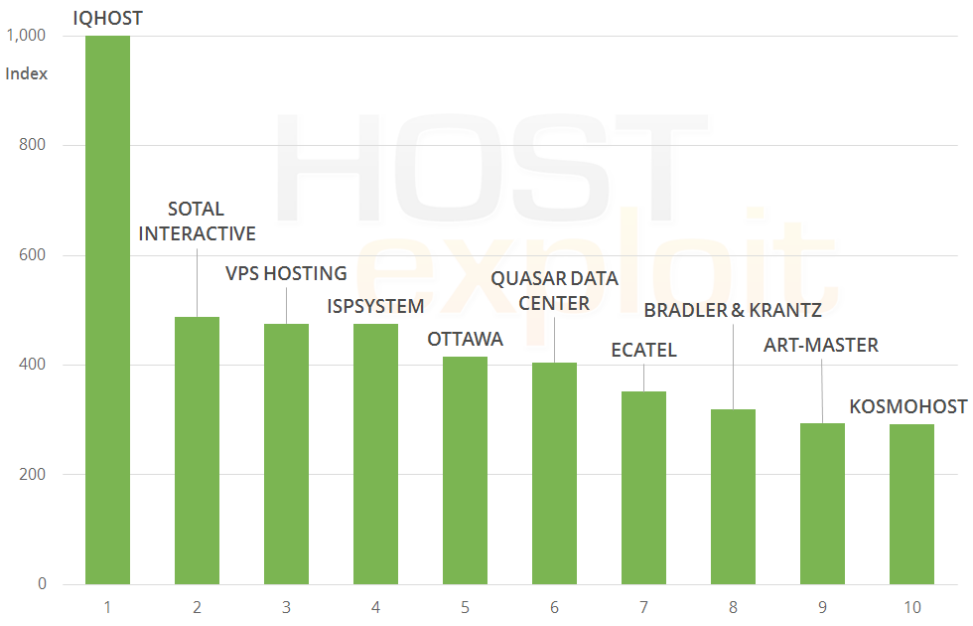
Ни одна из первых четырех позиций в этой категории не изменилась по сравнению с отчетом за первый квартал 2013 года.

Более того, AS50465 IQHost возглавляет рейтинг еще со второго квартала 2012 года. Таким образом, он уже более чем год является хостом №1 для C&C ботнетов.

Статистика

За указанный период было обнаружено 124 командных центра, в отличие от 132, обнаруженных за прошлый период.

В сумме этот показатель меньше, нежели вредоносная активность, зафиксированная в любой другой категории. Однако мощь каждого из подобных командных центров, подчеркивает важность их изучения и анализа с точки зрения безопасности.

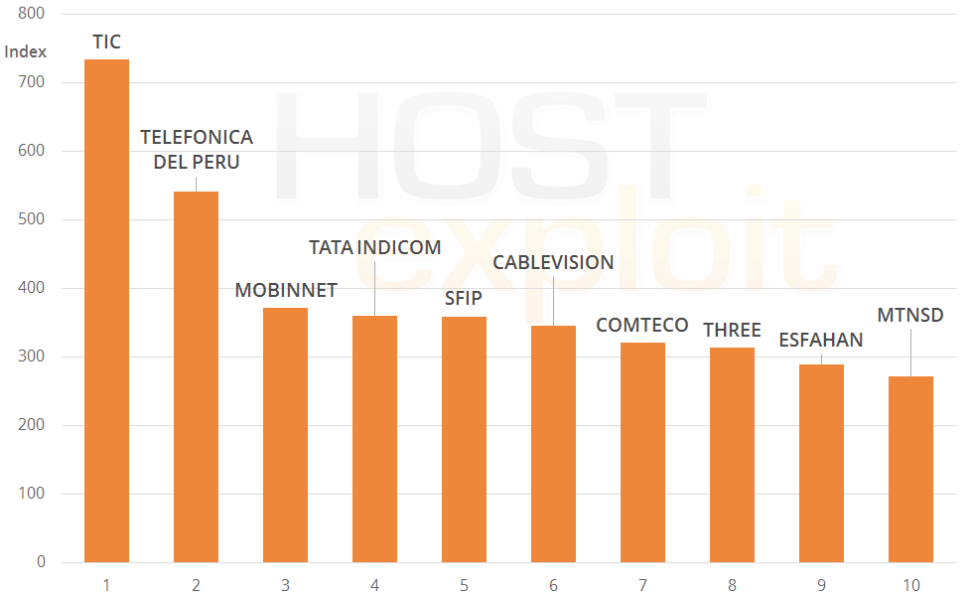


Спам

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
733.8	48159	Telecommunication Infr...	IR	192,256	23	150.7
541.4	6147	Telefonica del Peru	PE	2,048,768	39	122.6
371.1	50810	Mobin Net Communication	IR	230,400	228	68.7
360.1	55740	Tata Indicom	IN	262,144	244	66.7
358.9	57879	sfip84	DE	5,120	242	66.8
345.4	28548	Cablevisión, S.A. de C.V.	MX	147,968	274	64.0
320.2	27839	Comteco Ltda	BO	47,616	336	59.4
313.1	45727	Three Hutchison	US	14,400	354	58.2
288.4	58085	Esfahan Telecommunication	IR	131,072	437	53.5
271.0	36972	MTNSD	SD	3,328	488	50.5

Первые позиции в этой категории следуют тенденции, вырисовавшейся в предыдущих отчетах. Спаммеры продолжают отдавать предпочтение странам с наиболее слабыми законодательными ограничениями и наименьшими барьерами на пути регистрации автономных систем.

Под это описание подходят 8 из 10 первых хостов – здесь представлены Иран, Перу, Мексика, Индия и Боливия. Исключениями являются AS57879 SFIP, зарегистрированный в Германии, и AS45727 Three, который находится в США, хоть и зарегистрирован в Индонезии.



Что мы делаем?

В данной категории мы рассматриваем традиционные спам-сервера, а также спам-боты, сканеры и репутацию общественных IP-адресов.

Знаете ли Вы?

Российский телекоммуникационный провайдер «Мегафон», наконец-то вышел из Top 10. В 2012 году у провайдера насчитывалось целых четыре АС, которые входили в Top 10 категории Спам.

Статистика

За данный отчетный период было исследовано и проанализировано более 100,000 источников спама.

Знаете ли Вы?

По оценкам Cisco, в 2012 году у корпораций и потребителей с помощью фишинг-атак было украдено около 100 миллиардов долларов.

Статистика

За данный отчетный период было исследовано 779 уникальных фишинг-кампаний.

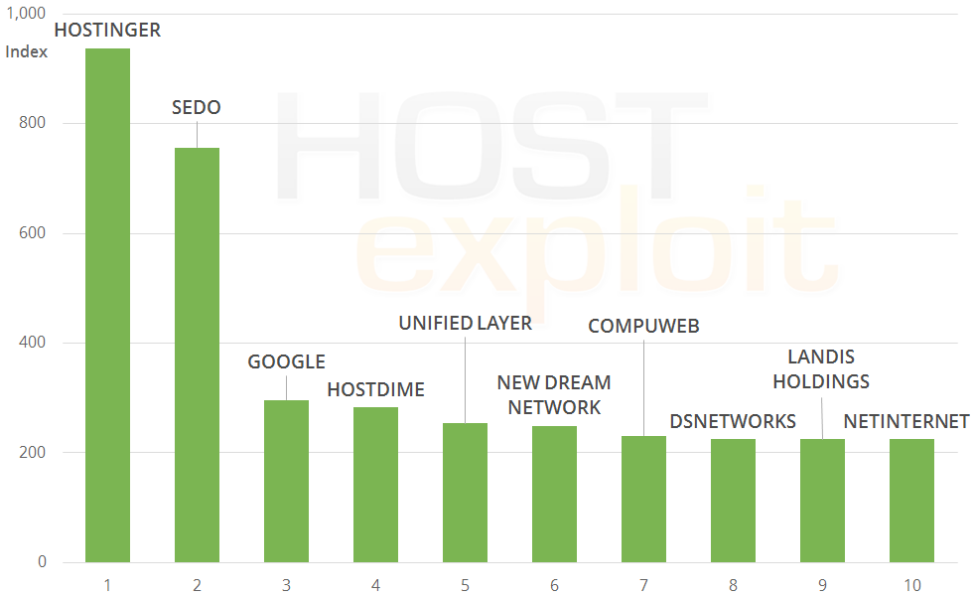
Фишинг

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
937.3	47583	Hostinger International	US	11,008	11	194.5
756.3	47846	Sedo GmbH	DE	1,280	229	68.1
296.4	15169	Google Inc.	US	669,696	42	120.2
282.9	33182	HostDime.com, Inc.	US	63,232	1	252.3
253.2	46606	Unified Layer	US	508,416	17	174.7
248.7	26347	New Dream Network, LLC	US	230,656	2	249.3
230.9	15510	Compuweb Comms...	GB	6,912	78	102.5
225.2	46816	DirectSpace Networks, LLC.	US	8,192	578	47.0
225.0	11042	Landis Holdings Inc	US	28,416	3	243.5
224.2	51559	Netinternet	TR	18,432	25	149.3

В Топ-10 данной категории лидируют хостинговые компании из стран с развитым законодательством – в том числе ранее упоминавшиеся 3 «самых плохих» хоста.

В этом изменчивом секторе фишеры предпочитают простоту и доступность хостинга в развитых регионах. Поскольку жизнь фишинговых сайтов коротка, гарантии длительной работоспособности не требуются, а значит, не нужно искать регионы, в которых отсутствует соответствующее законодательство.

Поэтому возрастающее доверие к сайтам по банкингу и электронной коммерции, размещенных в США и Великобритании, является выгодным для мошенников, занимающихся фишингом.

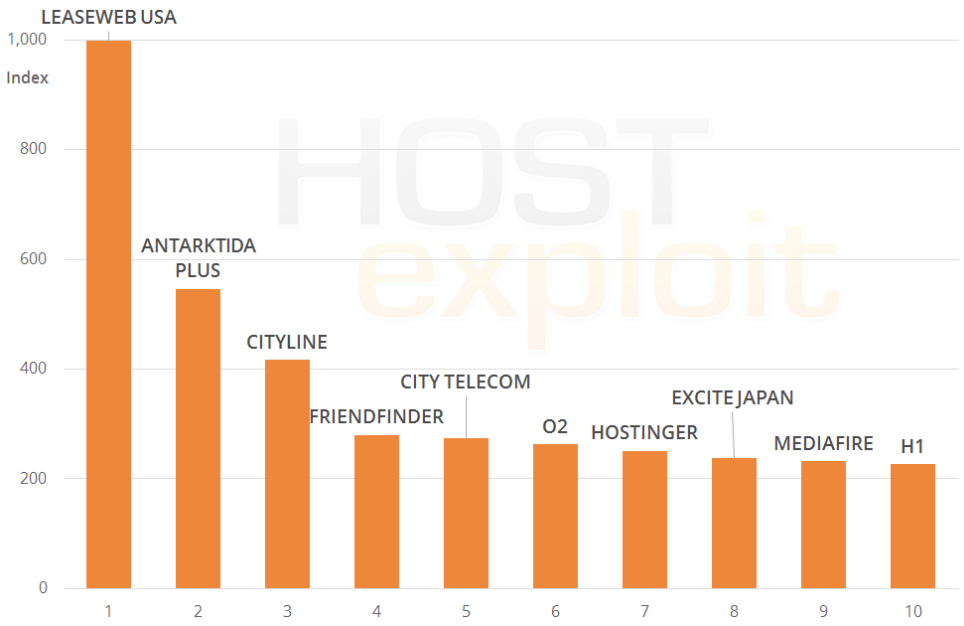


Текущие события

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
998.6	30633	Leaseweb USA	US	14,592	16	178.0
545.8	51699	Antarktida-Plus	SC	256	305	61.6
417.0	34023	PE Shattah Zia G.Naman	EU	256	283	63.3
280.2	32527	FriendFinder Networks	US	2,560	1,008	32.0
273.9	48271	City Telecom	KG	8,192	51	115.5
262.3	31080	o2 Sp. Z.o.o.	PL	512	311	61.2
251.3	47583	Hostinger International	US	11,008	11	194.5
237.2	45682	Excite Japan Co., Ltd.	JP	2,048	1,267	27.3
231.5	46179	MediaFire, LLC	US	3,072	1,320	26.6
227.0	6870	H1 LLC	RU	5,632	1,383	26.0

AS51699 Antarktida снова занимает высокую позицию в данной категории, однако возглавляет рейтинг в этот раз AS30633 Leaseweb USA.

Как следует из самого названия, «текущие события» – это быстро изменяющийся сектор, а значит, для новых видов вредоносной деятельности используются новые хосты, что влечет за собой значительные изменения от месяца к месяцу.



Знаете ли Вы?

«Текущие события»– это исследование компании HostExploit, посвященное самым современным и быстроменяющимся атакам со всего мира.

В список включены различные варианты MALfi-атак (XSS\/ДВ\/RFI\/LFI), clickjacking атаки и большие бот-сети.

Статистика

После некоторого спада количества случаев вредоносной активности, отмеченного в предыдущем периоде, эта цифра снова увеличилась на целых 67%.

Знаете ли Вы?

Zeus - вид ботнета, который заражает машины пользователей с помощью payload трояна. Он остается одним из самых популярных видов ботнета уже на протяжении 6 лет.

Zeus постоянно улучшается, и имеет много вариаций, каждая из которых способна обойти системы безопасности и превратить в «зомби» большое количество машин.

Статистика

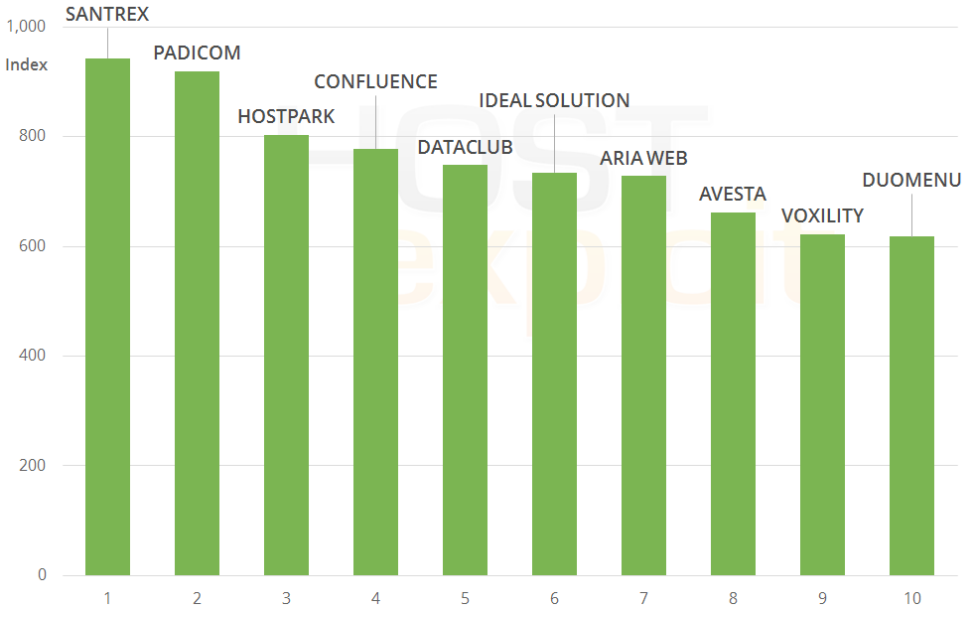
Общее количество серверов Zeus за год осталось практически неизменным. Данный факт свидетельствует о том, что Zeus по-прежнему остается успешным и прибыльным инструментом для создания ботнетов.

Ботнеты Zeus

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
942.9	57668	Santrex Internet Services	SC	5,632	38	124.4
919.6	34201	Padicom Solutions SRL	RO	6,400	76	102.9
803.6	51743	PE Taran Marina Vasil'evna	UA	256	107	92.2
778.0	40034	Confluence Networks Inc	VG	12,288	10	195.7
748.7	52048	DataClub S.A.	LV	2,048	97	95.4
734.7	58001	Ideal Solution Ltd	RU	2,560	35	126.3
727.9	57230	Aria Web Development LLC	GB	2,816	62	109.6
662.0	54444	Avesta Networks LLC	US	5,632	77	102.9
622.2	39743	Voxility S.R.L.	RO	55,808	19	162.0
618.0	16125	UAB Duomenu Centras	LT	7,936	123	85.8

Первую позицию здесь занимает AS57668 Santrex, у которого есть одна сходная черта с №1, засветившегося в первом квартале 2013 года – он тоже маршрутизируется через Сейшелы.

В предыдущем отчете верхнюю позицию занимал AS58001 Ideal Solution, который сейчас на 5-м месте; он зарегистрирован на Сейшелах, но маршрутизируется через Российскую Федерацию.

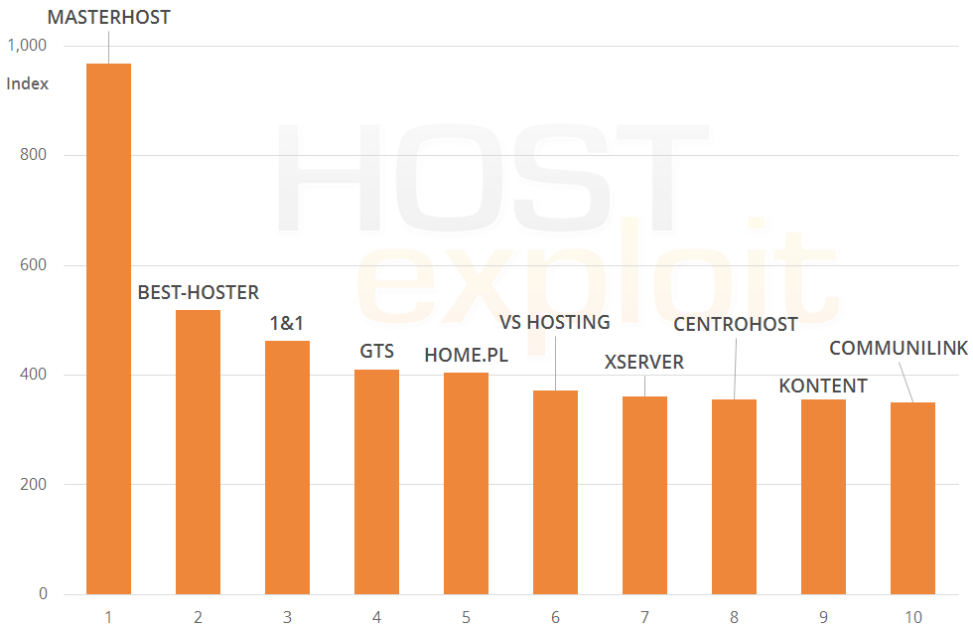


Эксплоиты

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
968.4	25532	Masterhost	RU	77,824	12	193.0
517.9	49693	Best-Hoster Group Co. Ltd	RU	2,048	70	105.5
462.1	8560	1&1 Internet AG	DE	370,176	9	198.7
410.1	8358	GTS Hungary	HU	30,720	41	120.6
404.4	12824	home.pl	PL	204,800	13	191.6
371.2	43541	VSHosting s.r.o.	CZ	14,336	155	79.1
361.7	48031	PE Ivanov Vitaliy Sergeevich	UA	15,616	47	116.8
355.5	41126	JSC Centrohost	RU	4,096	33	130.2
355.5	24973	KONTENT GmbH	DE	4,096	196	73.4
350.3	38277	CommuniLink Internet	HK	4,608	230	68.0

В данной категории имеются «нарушители-рецидивисты»: AS25532 Masterhost и AS49693 Best-Hoster, которые появлялись здесь ранее.

Однако, большинство хостинг-компаний данной категории являются новичками в этом секторе.



Знаете ли Вы?

Эксплоиты и веб-сайты, на которых они находятся, являются ключевой частью головоломки всех киберпреступлений, поскольку именно они чаще всего являются отправной точкой для получения доступа к компьютеру жертвы.

Эксплоиты используют как неизвестные так и публично доступные уязвимости в программном обеспечении. Эксплоит может содержать код, который приносит вред непосредственно системе жертвы, или же могут быть использованы злоумышленником в качестве лоадера (payload), для получения управления над компьютером жертвы.

Статистика

AS, которые входят в Top 10 данной категории , содержат более 16% от общего количества эксплоитов, исследованных за период подготовки исследования, в отличии от 29% за прошлый период.

Знаете ли Вы?

Вредоносное программное обеспечение, как правило, не учитывает, для каких целей пользователь использует свой компьютер. Примерами такого ПО являются шпионские программы, различные виды хакерских программ, а также замаскированное рекламное ПО. Обычно они проявляются в виде бесплатных заставок, которые скрыто создают рекламные объявления, перенаправляют браузеры на посторонние вэб-страницы, в то время как килоггеры перенаправляют личные данные пользователя третьим лицам, которые являются злоумышленниками.

Статистика

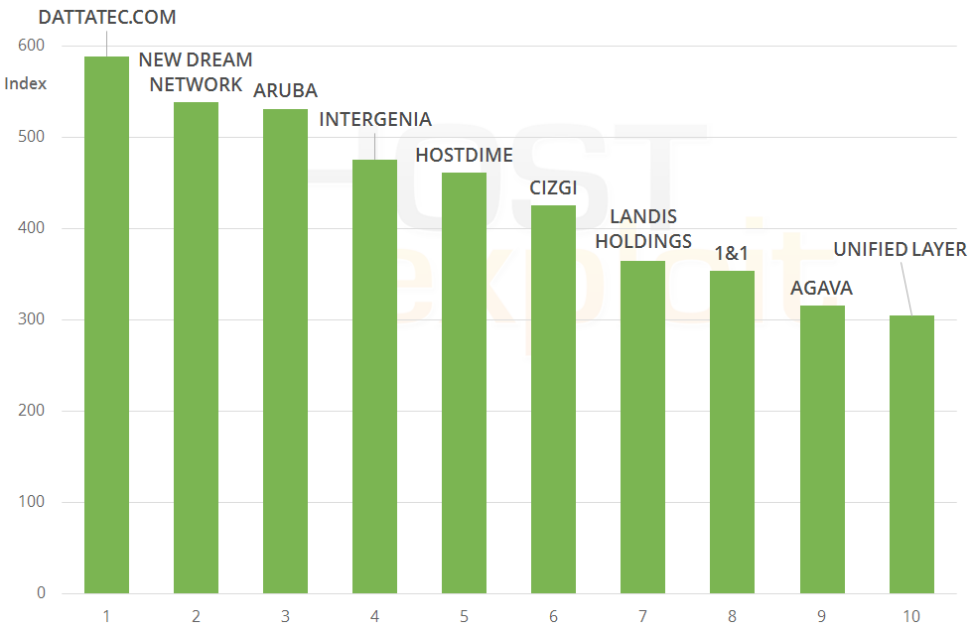
Топ 10 хостов в этой категории отвечают за 23% всех наблюдавшихся случаев вредоносной активности.

Вредоносные программы

Индекс	#AS	Название	Страна	IPs	Рейтинг	Индекс НЕ
588.4	27823	Dattatec.com	AR	8,192	4	226.8
538.7	26347	New Dream Network, LLC	US	230,656	2	249.3
531.0	31034	Aruba S.p.A.	IT	145,664	7	213.6
475.6	8972	Intergenia AG	DE	149,760	6	219.6
461.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
425.0	34619	Cizgi Telekomunikasyon	TR	30,208	14	184.5
364.8	11042	Landis Holdings Inc	US	28,416	3	243.5
353.2	8560	1&1 Internet AG	DE	370,176	9	198.7
315.7	43146	Agava Ltd.	RU	19,712	8	201.2
304.5	46606	Unified Layer	US	508,416	17	174.7

В этом изменчивом секторе только два хоста остались неизменными по сравнению с первым кварталом – это AS31034 Aruba и AS8560 1&1 Internet. ВЗловредное ПО зависит от кратковременных трендов, и поэтому вполне естественно, что игроки данной категории меняются быстро.

Тройка «худших» хостов имеет высокий рейтинг не только в этой категории, но и по фишингу и инфицированным веб-сайтам. Это свидетельствует о том, что серверы для вредоносной деятельности во всех этих категориях выбираются по сходным критериям.



Автономная система (Autonomous System)

Система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом. Уникальный номер AS (или ASN) присваивается каждой АС для использования в BGP маршрутизации. Номера АС в BGP очень важны, так как именно ASN однозначно идентифицирует каждую сеть в Интернете. На середину 2011 года в глобальной таблице маршрутизации представлено более 37 тысяч автономных систем.

Вредоносное программное обеспечение (Badware)

Программное обеспечение, которое принципиально игнорирует выбор пользователя в отношении того, как его компьютер будет использоваться. Типичными примерами вредоносного программного обеспечения могут быть бесплатные заставки, которые генерируют скрытую рекламу, вредоносные панели инструментов веб-браузеров, которые перенаправляют ваш браузер на страницу, отличную от той, которую вы ожидали, и клавиатурные шпионы, которые могут передавать ваши персональные данные злоумышленникам.

«Черные списки» (Blacklists)

В программировании «черный список» это основной механизм контроля доступа, который позволяет получить доступ так же, как если бы это был обычный ночной клуб; допускается все, кроме людей, которые находятся в черном списке. Противоположностью этому является «белый список», эквивалентной вашему VIP-клубу, что значит не пускать никого, кроме тех, кто состоит в белом списке. Чем-то средним является «серый список», содержащий записи, которые временно заблокированы или временно разрешены. Элементы «серого списка» могут быть пересмотрены в дальнейшем для включения в «черный» или в «белый список». Некоторые сообщества и веб-разработчики, такие как Spamhaus и Emerging Threats, публикуют свои «черные списки» для их дальнейшего использования широкой общественностью.

Ботнет (Botnet)

Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используются для нелегальной деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании.

Межсайтовая подделка запроса (CSRF)

Также известна как «атака в один клик» / управление сессией, которая может быть ссылкой или скриптом на веб-странице и основывается на получении подлинной авторизации пользователя.

Система доменных имен (DNS)

Компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене. Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Черный список DNS (DNSBL)

Списки хостов, хранимые с использованием системы архитектуры DNS. Обычно используются для борьбы со спамом. Почтовый сервер обращается к DNSBL и проверяет в нем наличие IP-адреса клиента, с которого он принимает сообщение. При положительном ответе считается, что происходит попытка приема спам-сообщения. Серверу отправителя сообщается ошибка 5xx (неустранимая ошибка) и сообщение не принимается. Почтовый сервер отправителя создает «отказную квитанцию» отправителю о недоставке почты.

Эксплойт (Exploit)

Это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования (DoS-атака).

Хостинг (Hosting)

Услуга по предоставлению вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети (обычно Интернет). Обычно под понятием услуги хостинга подразумевают как минимум услугу размещения файлов сайта на сервере, на котором запущено ПО, необходимое для обработки запросов к этим файлам (веб-сервер). Как правило, в услугу хостинга уже входит предоставление места для почтовой корреспонденции, баз данных, DNS, файлового хранилища и т. п., а также поддержка функционирования соответствующих сервисов.

IANA

IANA отвечает за общую координацию DNS значения, IP-адресации, и других интернет-ресурсов. Она координирует пространство IP-адресов, и выделяет их региональным интернет-регистраторам.

ICANN

ICANN отвечает за управление адресным пространством интернет протокола (IPv4 и IPv6) и присвоение адресных блоков региональным интернет-регистраторам для поддержания регистраторов идентификаторов интернет протокола, а также за управление пространством доменных имен верхнего уровня (корневой зоны DNS).

IP (Internet Protocol)

Маршрутизируемый сетевой протокол, протокол сетевого уровня семейства TCP/IP. Протокол IP используется для негарантированной доставки данных, разделяемых на так называемые пакеты от одного узла сети к другому. Это означает, что на уровне этого протокола (третий уровень сетевой модели OSI) не даётся гарантий надёжной доставки пакета до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (когда приходят две копии одного пакета; в реальности это бывает крайне редко), оказаться повреждёнными (обычно поврежденные пакеты уничтожаются) или не прибыть вовсе. Гарантию безошибочной доставки пакетов дают протоколы более высокого (транспортного уровня) сетевой модели OSI — например, TCP — которые используют IP в качестве транспорта.

IPv4

Интернет-протокол версии 4 (IPv4) является четвертой переработкой в развитии Интернет-протокола (IP). IPv4 использует 32-разрядный (четыре байта) адрес, который ограничивает адресное пространство до 4,3 миллиардов возможных уникальных адресов. Тем не менее, некоторые из них зарезервированы для специальных целей, таких как частные сети (18 млн.), или широковещательные адреса (270 млн.).

IPv6

Интернет-протокол версии 6 (IPv6) представляет собой версию интернет-протокола, который предназначен для смены IPv4. IPv6 использует 128-битный адрес, адресное пространство IPv6 поддерживает около 2 ^ 128 адресов.

Интернет-провайдер (ISP)

Компания или организация, которая имеет оборудование и возможность для обеспечения подключения к сети Интернет-клиентов на платной основе, обеспечение доступа к электронной почте, серфингу веб-сайтов, онлайн-хранению данных.

LFI (Local File Inclusion)

Использование файла внутри базы данных для использования функций сервера. Также используется для взлома зашифрованных функций сервера, например: паролей, MD5 и т.д.

MALfi (Malicious File Inclusion)

Сочетание RFI (remote file inclusion), LFI (local file inclusion), XSA (cross server attack) и RCE (remote code execution).

Вредоносные ссылки (Malicious Links)

Это ссылки, которые размещаются на сайте для того чтобы намеренно отправить посетителей на вредоносный сайт, например, сайт, на котором размещены вирусы, программы-шпионы или любой другой тип вредоносных программ, такие как поддельные системы безопасности. Неверная переадресация пользователю не всегда очевидна, так как они могут использовать особенности сайта или замаскировать свою деятельность.

MX

Почтовый сервер или компьютер / серверная стойка, который содержит и может пересылать электронную почты для клиента.

NS (Name Server)

Название записи в DNS, указывающей на DNS-сервер (сервер имен) для данного домена; либо сокращенное наименование собственно DNS-сервера.

Open Source Security

Термин чаще всего применяется к исходному коду программного обеспечения или данным, которые становятся доступными для широкой публики с послаблением или вообще отсутствием ограничений интеллектуальной собственности. Open Source Security позволяет пользователям создавать пользовательский программный контент и поддерживать его с помощью собственных усилий и путем взаимодействия с другими пользователями.

Фарм-бизнес (Pharming)

Это хакерская атака, целью которой является перенаправление трафика одного веб-сайта на другой сайт. Конечные сайты, как правило, поддельные и созданы с целью реализации контрафактных медикаментов.

Фишинг (Phishing)

Фишинг является одним из видов обмана, целью которого является получение доступа к конфиденциальным данным, таким как номера кредитных карт, пароли, данные по счетам или другая информация. Фишинг, как правило, осуществляется с использованием электронной почты (где сообщение исходит, якобы, от доверенных лиц), а также личных сообщений внутри различных сервисов, например, от имени банков.

Регистрация доменных имен (Registry)

Регистратор генерирует так называемые файлы зон, которые сопоставляют имена доменов IP-адресам. Например, регистраторы доменных имен: VeriSign для зоны .com и Afilias для зоны .info. Национальный домен верхнего уровня (ccTLD) предоставляются администратором национального домена, таким как Nominet в Соединенном Королевстве для .UK или «Координационный центр национального домена. RU» для. RU и. РФ.

Регистратор доменных имен (Registrars)

Это компания с полномочиями регистрации доменных имен, уполномоченная ICANN.

Remote File Inclusion (RFI)

Метод, часто используемый для атак интернет-сайтов с удаленного компьютера. Он может быть объединен с использованием XSA для нанесения вреда веб-серверу.

Мошенническое программное обеспечение (Rogue Software)

Это программное обеспечение, использующее различные вредоносные инструменты для распространения рекламы или побуждения пользователей платить за удаление несуществующих программ-шпионов и блокираторов. Мошенническое программное обеспечение часто устанавливает троянские программы для выполнения несанкционированных действий.

Rootkit

Набор программных инструментов, используемых третьим лицом после получения доступа к компьютерной системе, для сокрытия изменений файлов или процессов, которые выполняются третьими лицами без ведома пользователя.

Sandnet

Это закрытая компьютерная среда, в которой можно наблюдать и изучать вредоносную программу. Она эмулирует Интернет таким образом, что вредоносное ПО не поймет, что за ним наблюдают. Важна для анализа того, как работает вредоносная программа. Honeynet имеет такую же концепцию, но больше нацелен на самих атакующих, позволяя наблюдать и изучать их методы и мотивы.

Спам (Spam)

Массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений (информации) лицам, не выражавшим желания их получать.

Троян (Trojans)

Также известен как троянский конь. Это программа, которая выполняет вредоносные задачи без ведома и согласия пользователя.

Червь (Worms)

Вредоносная программа, которая может воспроизводить себя и передаваться по сети от одного компьютера на другой. Разница между червем и компьютерным вирусом состоит в том, что компьютерный вирус для распространения прикрепляется к компьютерной программе и требует действий со стороны пользователя, в то время как червь является автономным и может отправлять копии по Сети.

XSA (Cross Server Attack)

Метод вторжения в сетевую безопасность, который позволяет злоумышленнику нарушить безопасность веб-сайта или сервиса на сервере с помощью незащищённых функций, реализуемых на нем.

Приложение 2

1 Последовательность изменений

Поправка	Дата	Примечание
1.	Декабрь 2009	Внедрение методологии .
2.	Март 2010	Количество IP-адресов выросло с 10,000 до 20,000.
3.	Июнь 2010	Увеличено количество источников. Двойная обработка данных о безопасности просмотра информации в системе Google была устранена посредством механизма StopBadware. Усовершенствована оценка источников
4.	Октябрь 2011	Увеличено количество источников. Усовершенствована оценка источников.
5.	Июль 2012	Увеличено количество источников.

Таблица 1: Последовательность изменений

2 Мотивация

Мы хотим показать простой и точный метод представления эволюции уровня зараженности на примере Автономных систем (АС). В данном контексте зараженность включает в себя вредоносную и подозрительную активность сервера, такую как хостинг и распространение вредоносного программного обеспечения и эксплойтов, рассылка спама, атаки MALfi, командные и управляющие центры ботнетов, фишинговые атаки.

Мы разработали Индексом НЕ — значение от 0 (зараженность отсутствует) до 1000 (максимальный уровень зараженности). Желаемые свойства Индекса НЕ включают в себя следующее:

1. Подсчеты должны проводиться на основе нескольких источников информации, каждый из которых должен представлять собой различные формы зараженности, чтобы уменьшить влияние любых отклонений информации.
2. При каждом подсчете должно учитываться некоторый реальный размер АС, так чтобы индекс был справедлив не только для небольших АС.
3. Ни одна АС не должна иметь Индекс НЕ равный 0, так как нельзя определенно сказать, что АС имеет нулевой уровень зараженности только лишь потому, что ни один вредоносный случай не был обнаружен.
4. Только одна АС должна иметь максимальное значение Индекса НЕ равное 1,000 (если она вообще существует).

3 Источники информации

Данные получены из следующих 11 источников.

№ п/п	Источник	Данные	Значимость
1.	UCEPROTECT- Network	Спам-серверы	Очень высокая
2.	Abuse.ch	Сервера ZeuS	Высокая
3.	Google / C-SIRT	Образцы вредоносного ПО	Очень высокая
4.	SudoSecure / HostExploit	Спам-боты	Средняя
5.	Shadowserver / HostExploit / SRI	Командные и управляющие сервера	Высокая
6.	C-SIRT / HostExploit	Сервера фишинга	Средняя
7.	C-SIRT / HostExploit	Сервера с эксплойтами	Средняя
8.	C-SIRT / HostExploit	Сервера для рассылки спама	Низкая
9.	«HostExploit»	Текущие события	Высокая
10.	hpHosts	Образца вредоносного ПО	Высокая
11.	Clean MX / C-SIRT	Вредоносные URL	Высокая
12.	Clean MX	Вредоносные шлюзы	Средняя

Таблица 2: Источники информации

Данные о рассылке спама, полученные из UCEPROTECT-Network, и данные о вредоносной программе ZeuS от Abuse.ch пересекаются со сведениями от организации Team Cymru.

Использование информации от этих многочисленных источников удовлетворяет необходимому свойству № 1.

Был проведен тест на чувствительность, чтобы определить диапазон специальных коэффициентов, которые гарантируют, что известные зараженные АС могут находиться в критическом состоянии. Точное значение каждого коэффициента внутри определенного диапазона было впоследствии выбрано по нашему усмотрению, основанному на глубоком понимании наших исследователей значения каждого из источников. Такой подход гарантирует, что результаты объективны насколько это возможно при ограничении необходимых субъективных элементов для получения разумных результатов.

4 Соотношение Байеса

Как мы можем удовлетворить необходимому свойству № 2? А именно, как нужно рассчитать Индекс НЕ, чтобы справедливо отразить размер АС? Первой мыслью является поделить количество зарегистрированных случаев на значение, отражающее размер АС. Наиболее очевидно, что мы можем использовать количество доменов в каждой сети, как значение, отражающее размер АС, но возможно, что сервер может совершать вредоносную активность без единого зарегистрированного домена, как в деле со спам-хостингом McColo. Кроме того, было бы целесообразнее использовать размер диапазона IP-адресов (т. е. количество IP-адресов), зарегистрированного под АС с помощью соответствующего Регионального интернет-регистратора.

Однако, при подсчете соотношения количества случаев на IP-адрес отдельные инциденты на небольших серверах могут привести к искаженным результатам. Рассмотрим следующий пример:

Среднее количество спам-станций в пробном наборе: 50
Среднее количество IP-адресов в пробном наборе: 50,000
Среднее соотношение: 50 / 50,000 = 0.001
Количество спам-станций в примере: 2
IP-адресов в примере: 256
Соотношение в примере: 2 / 256 = 0.0078125

В этом примере, используя простой подсчет количества спам-станций, поделенных на количество IP-адресов, соотношение получается почти в восесь раз больше, чем среднее значение. Несмотря на то, что было зарегистрировано только 2 спам-станции, соотношение достаточно большое по сравнению с небольшим количеством IP-адресов в этой конкретной АС. Это вполне могут быть изолированные инциденты, следовательно необходимо довести соотношение до среднего независимо от небольшого числа IP-адресов.
Для этого используется соотношение Байеса как соотношение количества случаев к количеству IP-адресов. Соотношение Байеса рассчитывается следующим образом:

$$B = (\frac{M}{M+C}) \cdot \frac{N}{M} + (\frac{C}{M+C}) \cdot \frac{N_a}{M_a} \quad (1)$$

где:

B: *соотношение Байеса*

M: количество *IP-адресов, выделенных под данный номер АС*

M_a : *среднее количество IP-адресов, выделенных в пробном наборе*

N: *количество зарегистрированных случаев*

N_a : *среднее количество зарегистрированных случаев в пробном наборе*

C: *вес IP-адреса = 20,000*

На процесс доведения соотношения до среднего значения влияет тот факт, что ни у одной АС соотношение Байеса не может быть равным нулю в связи с уровнем неопределенности, основанном на количестве IP. Это отвечает требованиям необходимого свойства № 3.

5 Вычисления

Для каждого источника информации рассчитываются 3 показателя.

Чтобы нанести любое соотношение Байеса на шкалу, мы делим его на максимальное соотношение Байеса в пробном наборе, чтобы получить показатель C:

$$F_C = \frac{B}{B_m} \quad (2)$$

где:

B_m : *максимальное соотношение Байеса*

Были проведены тесты на чувствительность, которые показали, что в небольшом количестве случаев показатель C слишком благоприятствует маленьким АС. Поэтому логично включить показатель, использующий общее количество случаев, в противоположность соотношению инцидентов к размеру. Так формируется показатель A:

$$F_A = min\{\frac{N}{N_a}, 1\} \quad (3)$$

Он соответствует такому же формату, что и показатель C, и должен иметь лишь небольшое значение для Индекса, поскольку он стремится к малым АС и используется как механизм компенсации для редких случаев показателя C.

Если одна конкретная АС имеет некоторое количество станций, которое значительно выше, чем в любой другой АС из примера, тогда показатель A будет очень низким даже для АС со вторым по величине количеством станций. Это не желательно, так как значение для одной АС искажает значение показателя A. Следовательно, как компенсирующий механизм для показателя A (соотношение среднего количества случаев) используется показатель B в качестве отношения максимального количества случаев минус среднее количество:

$$F_B = \frac{N}{N_m - N_a} \quad (4)$$

где:

N_m : *максимальное количесвто станций в пробном наборе*

Показатель A ограничен до 1; Показатели B и C не ограничены до 1, поскольку они не могут превысить 1 по определению. Только одна АС (если такая имеется) может иметь максимальные значения всех трех показателей, по этой причине это приближает значение Индекса НЕ до 1,000, как указано в заданном свойстве № 4.

Индекс для каждого источника данных может быть рассчитан следующим образом:

$$I = (F_A \cdot 10\% + F_B \cdot 10\% + F_C \cdot 80\%) \cdot 1000 \quad (5)$$

Вес показателей A, B и C (10%, 10%, 80% соответственно) были выбраны на основании испытаний чувствительности и регрессии. Низкие начальные значения для показателя A и показателя B были выбраны, поскольку мы стремимся ограничить стремление к малым АС (свойство №2).

Общий НЕ-индекс далее рассчитывается как:

$$H = \frac{\sum_{i=1}^{11} I_i \cdot w_i}{\sum_{i=1}^{11} w_i} \quad (6)$$

где:

w_i : *вес источника (1=низкий, 2=средний, 3=высокий, 4=очень высокий)*