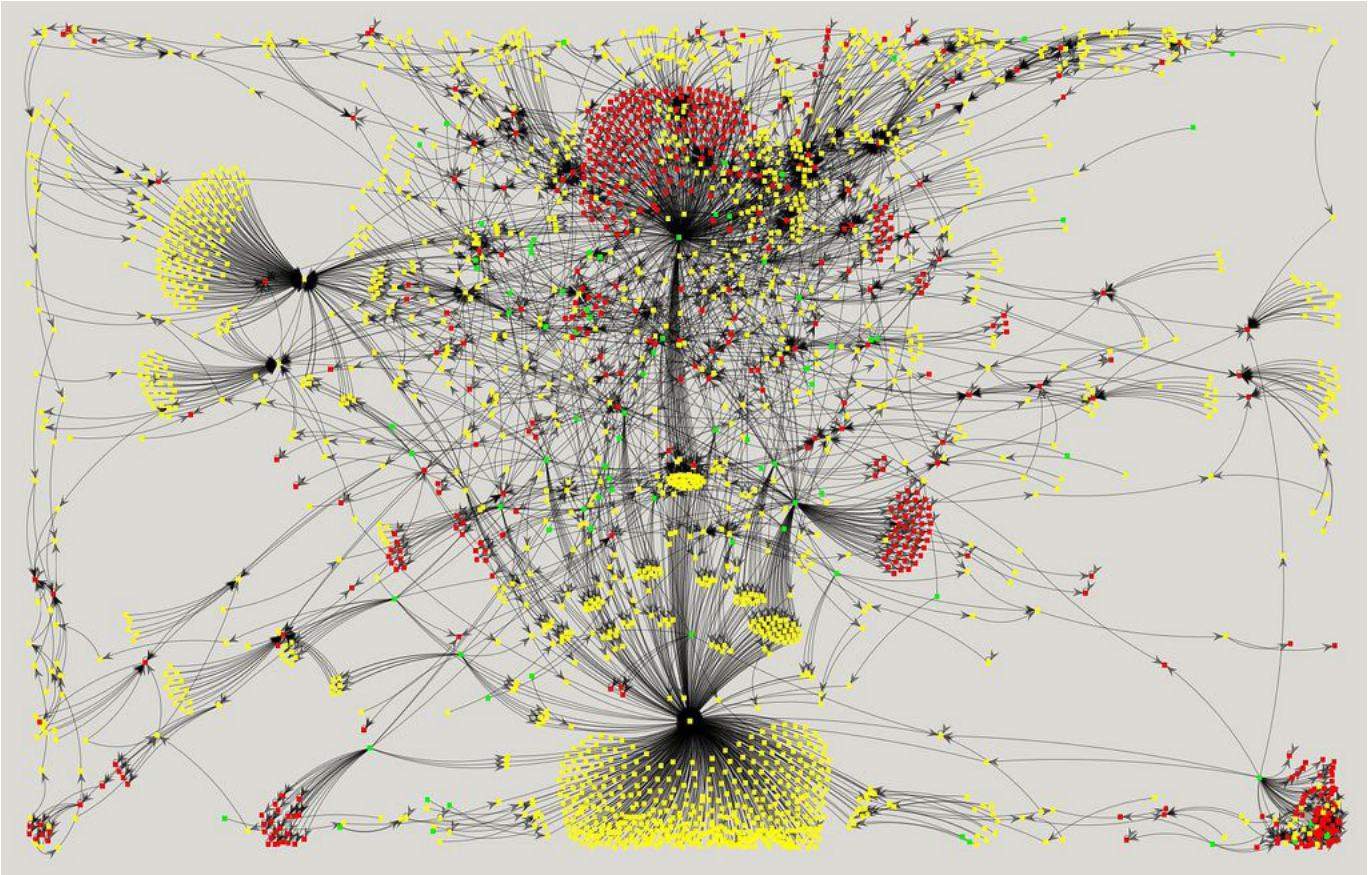
HostExploit Всемирный обзор кибепреступлений

Топ 50 «Самые плохие сети и хосты» IV квартал 2011

Отчет



Shnakule - Malware Delivery Network

SITEVET HOST exploit GROUP IB

Оглавление

1. Введение 4
2. Обзор последних событий 5
3. Часто задаваемые вопросы 7
4. Топ 50 8
5. Сравнение IV и III квартала 2011 года 9
6. График распределения Индекса НЕ 10
7. Новое за квартал 11
   - 7.1 Обзор 11
   - 7.2 Вновь зарегистрированные хосты 12
   - 7.3 Вылеченные хосты 13
   - 7.4 Хосты, состояние которых ухудшилось 14
8. Анализ по странам 15
9. «Чистые» хосты 16
10. Опасные хосты по категориям 17
    - 10.1 Серверы
      - 10.1.1 C&C-серверы 17
      - 10.1.2 Серверы фишинга 18
      - 10.1.3 Эксплойт серверы 19
      - 10.1.4 Серверы Zeus 20
    - 10.2 Направления деятельности
      - 10.2.1 Зараженные веб-сайты 21
      - 10.2.2 Спам 22
      - 10.2.3 Иные угрозы 23
      - 10.2.4 Вредоносное ПО 24
11. Выводы 25

Приложение 1 Словарь 26

Приложение 2 Методология 29

SITEVET HOST exploit GROUP IB

Топ 50

обзор кибепреступлений

Самые плохие сети и хосты

Supported by

nominet trust

www.nominettrust.org.uk

Редактор

- Jart Armin

Рецензенты

- Dr. Bob Bruen
- Raoul Chiesa
- Andre' DiMino
- Ilya Sachkov

Авторы

- Steve Burn
- Greg Feezel
- David Glosser
- Niels Groeneveld
- Tim Karpinsky
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson

Использованные источники

- AA419
- Abuse.CH
- CIDR
- Clean-MX.DE
- Emerging Threats
- Google Safe Browsing
- Group-IB
- HostExploit
- hpHosts
- ISC
- KnujOn
- MaliciousNetworks (FiRE)
- MalwareDomains
- MalwareDomainList
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- StopBadware
- SudoSecure
- Sunbelt
- Team Cymru
- UCE Protect

Front page illustration: Shnakule Malware Delivery Network - Courtesy BlueCoat

Введение

Введение

В рамках нашей инициативы по поддержке надежного хостинга мы представляем отчет Топ 50 «Самые плохие сети и хосты» по итогам IV квартала 2011 года. В число рейтинга вошли хосты, которые ненамеренно или намерено поддерживают вредоносную активность, угрожающую и вредящую пользователям Интернета во всем мире.

2011 год, характеризующийся слабой активностью некоторых организаций в области обеспечения собственной компьютерной безопасности, привел к шокирующему количеству утечек данных, порождающих все те же вопросы – кто, где и почему? Последний случай произошел в конце декабря – кража около 75 000 номеров кредитных карт у стратегического бюро прогнозов «Stratfor» сопровождалась публикацией в Сети более чем 850 000 имен и паролей доступа.

Совершенствуя нашу методологию распределения по странам, мы надеемся помочь выявить те регионы, где стандарты недостаточно проработаны, что обеспечивает безопасное существование киберпреступников. Оценка страны в рейтинге является более сложной процедурой, чем оценка конкретного хоста, и мы намерены продолжать работу в этом направлении. Соответствующий отчет будет опубликован в феврале — он будет посвящен результатам этой работы.

Определить принадлежность ресурсов в большинстве случаев практически невозможно, в связи с тем, что злоумышленники прячутся за отсутствием межгосударственного сотрудничества и международных стандартов в области интернет-технологий и компьютерной безопасности. Многие легко пользуются этой свободой, получая доступ к сервисам, позволяющим реализовать их преступные намерения.

Публикуя список хостов, на которых обнаружено наибольшее количество вредоносного контента за счет прямого использования их сервисов, мы надеемся стимулировать повышение ответственности хостинга, не доводя до необходимости вмешательства со стороны властей вплоть до принудительного отключения хостинга. В любом случае самостоятельное очищение гораздо лучше, чем жесткие действия органов правопорядка.

Те хосты, которые постоянно игнорируют необходимость действий, несмотря на очевидные данные, должны быть ликвидированы властями, так как граждане, использующие сервисы такого хоста, в действительности, только поддерживают дальнейшее развитие вредоносной активности. Отказываясь иметь дело с такими хостами, пользователи дадут понять, что иметь плохую репутацию экономически невыгодно.

Джарт Армин

(Jart Armin)

Обзор последних событий

«Карманный ботнет» / Pocket Botnet

«Карманный ботнет» представляет собой новую киберугрозу на фоне постоянно растущей популярности смартфонов. Злоумышленники все время ищут возможности получения прибыли за счет недостаточной защищенности телефонов большинства пользователей.

Предполагается, что в 2013 году количество используемых смартфонов превысит количество персональных компьютеров, составив около 2 миллиардов штук. Соответственно, смартфон станет наиболее предпочтительным устройством для выхода в Интернет.

В июне 2011 года International Data Corporation (IDC) сообщала, что к концу 2011 года поставки смартфонов вырастут до 450 000 единиц в год, а в дальнейшем достигнут миллиарда к 2015 году.

Данные, предоставленные Comscore, дополняют картину. Компания прогнозирует, что количество телефонов на платформе Android достигнет 50 % доли на рынке уже в 2012 году, так как к концу ноября прошлого года Android уже завоевала 46,9 % рынка. И поскольку потребители чаще останавливают свой выбор на телефонах с операционной системой Android, именно эта платформа становится целью для атак киберпреступников в погоне за наиболее прибыльным способом мошенничества.

Пользователи предпочитают удобство безопасности, и это создает массу возможностей для мошенников.

Например:

- До 50 % пользователей смартфонов работают с банковскими счетами через их устройство
- 97 % пользуются рабочим или личным почтовым ящиком
- 87 % телефонов предоставлены не работодателем
- Треть пользователей постоянно оставляют подключенными приложения/учетные записи

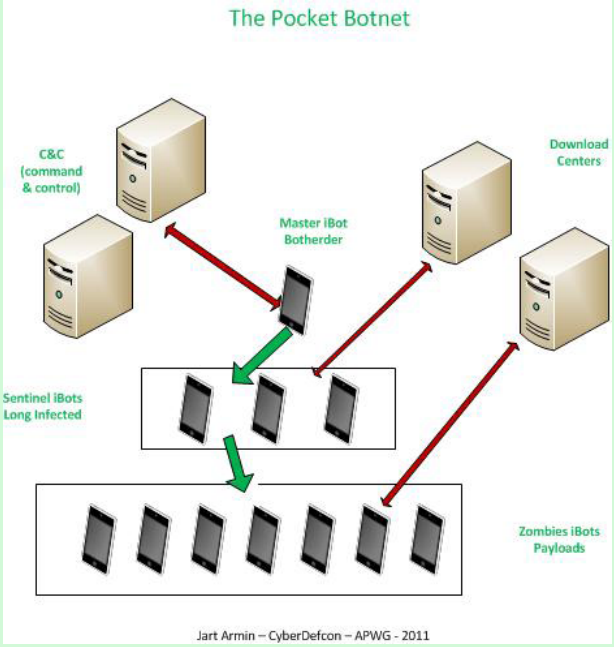
Источник: Confident Technologies

Неосторожные пользователи смартфонов продолжают обеспечивать относительный легкий доступ к устройству для целой армии вредоносных программ из арсенала киберпреступников. В настоящее время количество видов вредоносного ПО для смартфонов оценивается приблизительно в 1700, включая такие программы как Zitmo Android Edition (Zeus для мобильных телефонов), SpyEye, перехватывающий банковские SMS (mTANs), руткиты, средства для рассылки SMS на премиум-номера, шпионское ПО, инструменты для кражи данных, скликивания, DDoS-атак и другие вредоносные программы, распространяемые в Сети ежедневно.

Появление для смартфонов первых вредоносных программ с признаками наличия функционала для формирования ботнета дали ответ на вопрос о том, возможна ли мобильная версия ботнетов. Теперь важно понять, когда же они появятся в действительности.

Например, в семействе Android.SmsSend, количество модификаций которых за 2011 год возросло с 6 до 60, программа Answer.A самостоятельно устанавливает связь сервером управления.

А ThemeInstaller.A, по данным CnCert, заразил в Китае более одного миллиона смартфонов на платформе Symbian за одну неделю. Он имеет множество признаков программы-бота, включая сокрытие log-файлов, самоуничтожение, активность при отсутствии использования устройства, защиту от детектирования антивирусами и рассылку на другие смартфоны посредством СМС, а также загрузку нового вредоносного программного обеспечения с сервера управления.



Более 5700 достаточно активных ботнетов, существующих сегодня, открывают большие возможности для мошенников. В погоне за деньгами киберпреступники будут развивать новые навыки и технологии. Их целью будет любое устройство, которое напрямую или опосредованно подключается к сети Интернет. Смартфоны являются именно такими устройствами и пока еще предоставляют «плохим парням» возможность получить все, что они хотят.

Вышеизложенное является обновленным фрагментом из доклада «The Pocket Botnet», представленном на конференциях APWG eCrime 2011 в г. Сан Диего, США, и на UISG в г. Киев, Украина, в декабре 2011 г.

Группа DeepEnd Research

Созданная осенью 2011 года DeepEnd Research является независимой группой, занимающейся исследованиями в области информационной безопасности. Она была основана Андре М. Димино (Andre' M. DiMino) при участии Милы Паркур (Mila Parkour), Юрия Хвыля (Yuriy Khvyl), Джарта Армина (Jart Armin), Мэрни Кинг (Marnie King), Розанно Ферररис (Rosanno Ferraris) и Криса Ли (Chris Lee). Название группе дано не без доли иронии, так как каждый член группы может назвать по крайней мере один случай, когда исследование киберугроз привело его в глубокий, а иногда в очень даже мрачный омут.

На презентации сайта DeepEnd Research Андре М. Димино сказал:

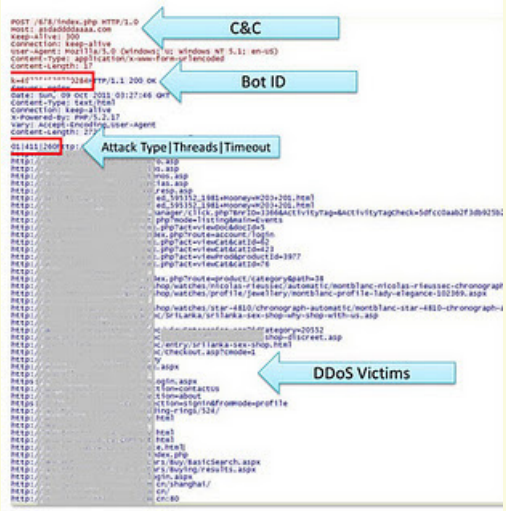
«Основной целью DeepEnd Research является стимулирование совместных исследований вместе с другими группами и организациями, занимающимися вопросами компьютерной безопасности».

Таким образом, группа остается гибкой в выборе объектов исследования и в методиках его проведения без каких-либо ограничений, которые могли бы быть привнесены другими «формализованными» организациями.

Каждый член другой группы привносит ценный опыт и профессионализм в активное изучение вредоносного программного обеспечения, анализ эксплойтов, отслеживание ботнетов, борьбу с черным ИТ-рынком и киберпреступностью в целом.

Бот для атак DDoS - Dirt Jumper

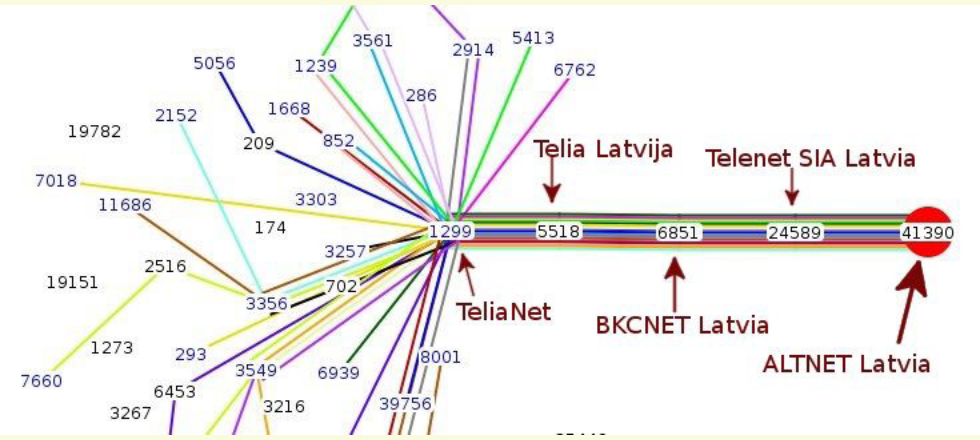
Предыдущее исследование нашей группы началось с первого знакомства с вредоносным программным обеспечением, демонстрировавшим признаки бота Dirt Jumper. Поиск по Message-Digest Algorithm (MD5) снова позволил выявить несколько серверов типа Command&Control и жертв атак класса DDoS.



Как выяснилось, многие антивирусные компании выявляли именно Dirt Jumper, но использовали различные имена для обозначения разновидностей одного и того же бота, например, такие как zbot, pinkslipbot, Kryptic, а Microsoft относит данное ПО к категории Dishigy.B. Но даже в этом случае исследователи смогли собрать большее количество примеров о результатах его деятельности.

Помимо идентификации разновидностей одного и того же бота, исследование выявило слабые места, которые могут препятствовать должному изучению вопроса. Очевидно, что основная проблема состоит в отсутствии стандартного подхода, например, при исследовании Dirt Jumper, и каждая компания, работающая в области компьютерной безопасности, использует собственную терминологию, давая самостоятельно имена обнаруженным вирусам. Поэтому тот же Dirt Jumper имеет много различных имен, что не только создает путаницу, но также может препятствовать всестороннему изучению проблемы.

Основным источником по данной теме является отчет SiteVet report on AS41390 RN-DATA / Altnet Latvi



Здесь приведен лишь краткий фрагмент из исследования Dirt Jumper. Полный текст с многочисленными иллюстрациями и диаграммами можно найти на сайте DeepEnd research.

Часто задаваемые вопросы

В 2009 году мы разработали Индекс НЕ — числовое представление уровня зараженности автономной системы (АС). Несмотря на то, что в целом данный индекс был хорошо принят профессиональным сообществом, с тех пор мы получили ряд важных вопросов, и на некоторые из них дадим ответы здесь.

Почему список показывает абсолютную зараженности, а не пропорциональную?

Ключевой характеристикой индекса является то, что он зависит от размера выделенного адресного пространства АС. И по этой причине он не отражает суммарную зловредную активность в информационной системе. Несомненно, статистика суммарной зараженности будет полезна для веб-мастеров и системных администраторов, которые могут ограничить количество нелегитимного траффика. Но Индекс НЕ предназначен для обнаружения случаев неприменения мер для обеспечения защиты среди хостинг-провайдеров по всему миру.

Должны ли крупные предприятия быть ответственны за инвестирование в доработку базы регулирования вопросов обеспечения безопасности?

Индекс НЕ более высок для АС с меньшим адресным пространством, но эта зависимость не линейна. Мы используем «фактор неопределенности» или фактор Баеса, чтобы смоделировать данную функцию, которая повышает значения для АС с большими адресными пространствами. В данном отчете критичный размер адресного пространства был увеличен с 10000 до 20000 для дальнейшего повышения данного эффекта.

Если данные показатели не для веб-мастеров, то для кого?

Данные отчеты рекомендованы к прочтению и для веб-мастеров, желающих получить понимание того, что происходит в мире информационной безопасности за пределами их повседневной жизни. Однако наша главная цель – повысить осведомленность об источниках проблем в области ИБ. Индекс НЕ определяет степень осуществления незаконной деятельности в сети организаций, которые, скорее всего, просто не в силах обнаружить, предотвратить и противостоять ей.

Почему данные хосты позволяют осуществлять зловредную деятельность?

Важно констатировать тот факт, что, опубликовав данные результаты, HostExploit не утверждает, что приведенные хостинг-провайдеры сознательно разрешают осуществление незаконной деятельности на своих серверах. Важно учитывать, что многие хосты являются жертвами киберпреступников, совершенно не зная этого. Именно в этом и заключается наша цель — предоставить своевременную информацию о степени зараженности тех или иных систем.

Обратная связь приветствуется!

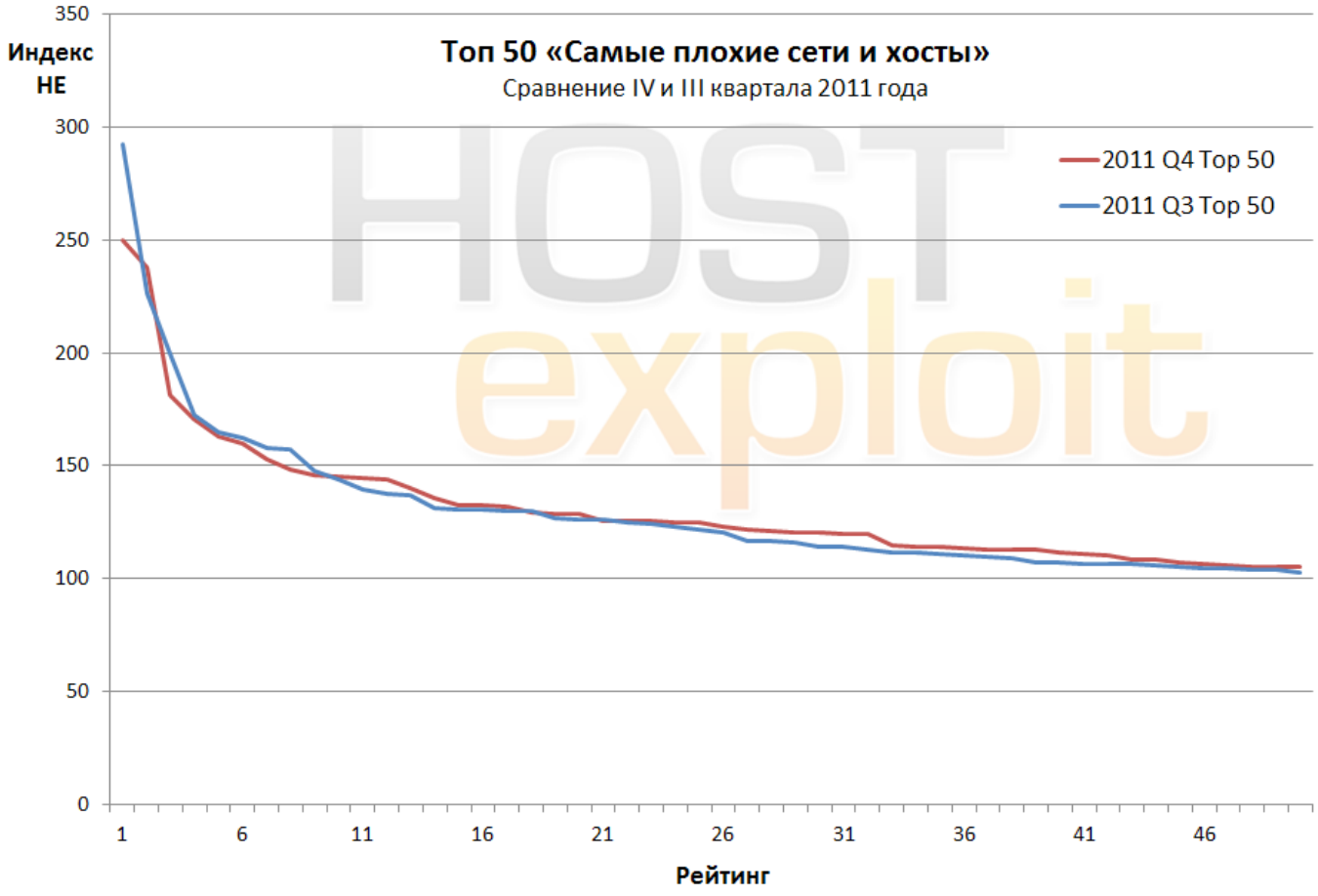
contact@hostexploit.com

info@group-ib.ru

4. Топ 50

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
▲ 1	249.90	47583	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	5,376
▲ 2	237.80	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	43,776
▶ 3	181.18	10297	ENET-2 - eNET Inc.	US	90,624
▲ 4	170.85	45634	SPARKSTATION-SG-AP 10 Science Park Road	SG	3,072
▲ 5	162.79	32475	SINGLEHOP-INC - SingleHop	US	248,064
▼ 6	160.09	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▲ 7	152.61	3595	GNAXNET-AS - Global Net Access, LLC	US	159,232
▲ 8	148.70	32613	IWEB-AS - iWeb Technologies Inc.	CA	235,776
▲ 9	146.10	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
▲ 10	144.95	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,541,376
▼ 11	144.64	16276	OVH OVH Systems	FR	583,168
▼ 12	144.19	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▼ 13	140.11	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,011,456
▲ 14	135.54	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA	IN	259,072
▲ 15	132.81	26347	DREAMHOST-AS - New Dream Network, LLC	US	329,216
▼ 16	132.40	22489	CASTLE-ACCESS - Castle Access Inc	US	49,408
▲ 17	132.15	24971	MASTER-AS Master Internet s.r.o	CZ	43,520
▲ 18	129.29	21788	NOC - Network Operations Center Inc.	US	281,088
▲ 19	128.67	8972	PLUSSERVER-AS intergenia AG	DE	147,456
▼ 20	128.48	24940	HETZNER-AS Hetzner Online AG RZ	DE	504,832
▲ 21	125.85	29873	BIZLAND-SD - The Endurance International Group, Inc.	US	96,768
▲ 22	125.82	45538	ODS-AS-VN Online data services	VN	9,472
▲ 23	125.35	6697	BELPAK-AS Republican Association BELTELECOM	BY	1,074,432
▼ 24	125.21	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,896
▲ 25	124.92	15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,928
▲ 26	122.93	36444	NEXCESS-NET - NEXCESS.NET L.L.C.	US	115,968
▼ 27	121.97	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	109,571,072
▼ 28	121.32	41947	WEBALTA-AS OAO Webalta	RU	15,872
▲ 29	120.74	9198	KAZTELECOM-AS JSC Kazakhtelecom	KZ	2,079,744
▼ 30	120.41	40824	WZCOM-US - WZ Communications Inc.	US	9,216
▼ 31	120.08	16265	LEASEWEB LeaseWeb B.V.	NL	281,344
▲ 32	119.64	31133	MF-MGSM-AS OJSC MegaFon	RU	19,456
▲ 33	114.46	25795	ARPNET - ARP NETWORKS, INC.	US	12,288
▲ 34	114.12	31147	INLINE-AS Inline Internet Online Dienste GmbH	DE	11,264
▼ 35	114.07	17971	TMVADS-AP TM-VADS Datacenter Management	MY	40,320
▲ 36	113.70	28753	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt)	DE	110,848
▲ 37	112.76	6939	HURRICANE - Hurricane Electric, Inc.	US	649,472
▲ 38	112.65	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▲ 39	112.63	47846	SEDO-AS Sedo GmbH	DE	1,280
▲ 40	111.87	9280	CIA-AS connect infobahn australia (CIA)	AU	8,704
▼ 41	111.18	9809	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	CN	10,496
▼ 42	110.17	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	131,840
▼ 43	108.43	15169	GOOGLE - Google Inc.	US	281,344
▼ 44	108.20	16125	DC-AS UAB Duomenu Centras	LT	5,376
▼ 45	107.15	43146	AGAVA3 Agava Ltd.	RU	17,408
▲ 46	106.48	40034	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	VG	3,328
▲ 47	105.62	44112	SWEB-AS SpaceWeb JSC	RU	3,072
▼ 48	105.38	9318	HANARO-AS Hanaro Telecom Inc.	KR	14,991,104
▲ 49	105.23	12260	COLOSTORE - Colostore.com	US	53,248
▲ 50	105.03	55330	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUNICATION	AF	16,384

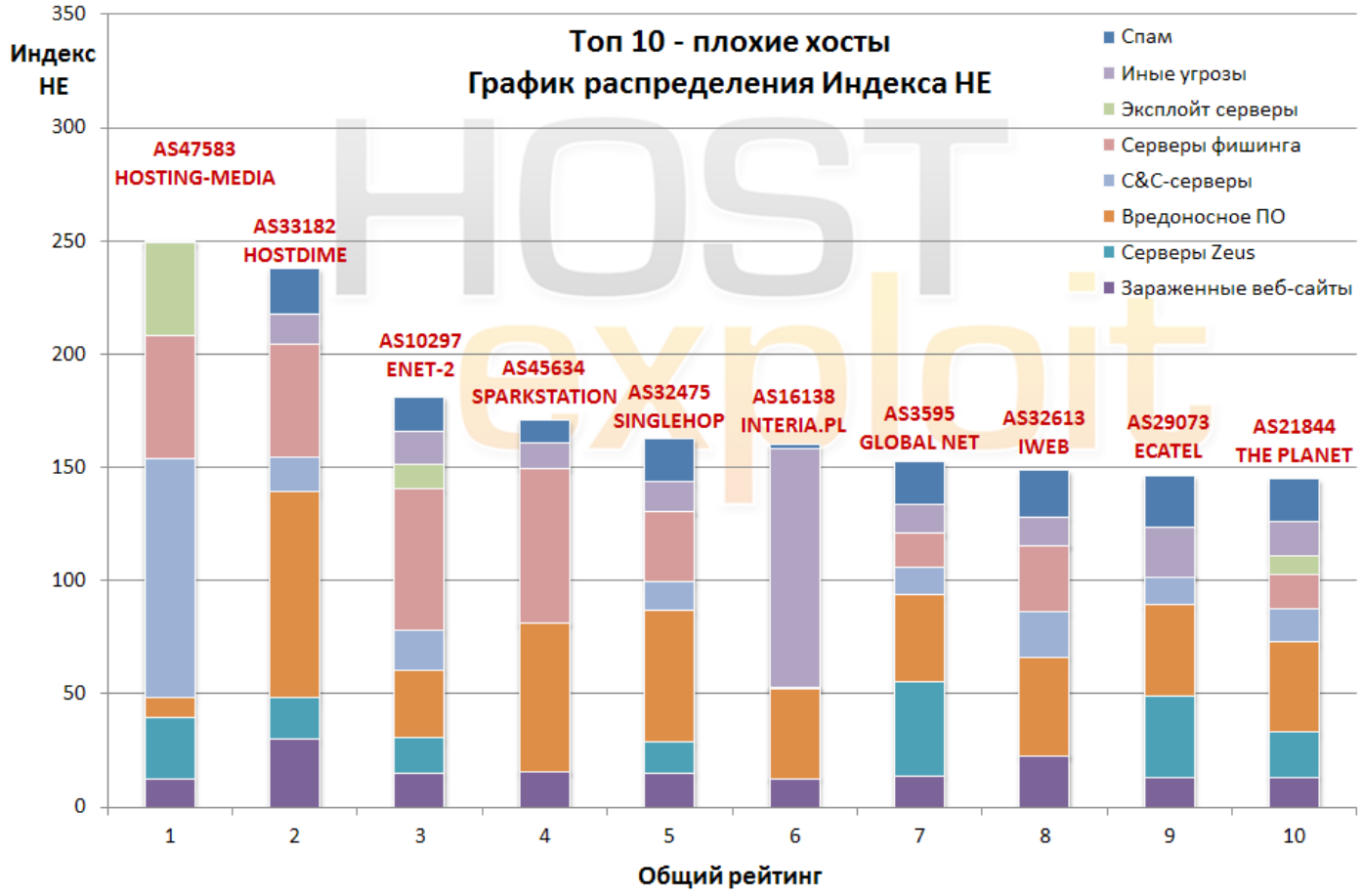
Сравнение отчетов за III и IV кварталы 2011



Сравнение отчетов Топ 50 «Самых плохих хостов», выпущенных в декабре 2011 года и в сентябре 2011 года.

Отчет за четвертый квартал отражает некоторые изменения уровня активности по сравнению с предыдущим временным периодом. В этом квартале меньшее количество хостов показало значительный рост в рейтинге, демонстрируя некоторое улучшение общей картины.

Топ 10. График распределения Индекса НЕ



Приведенная выше таблица иллюстрирует разбивку параметров для 10 худших хостов по Индексу НЕ.

Она демонстрирует эффективность применения взвешенных параметров в различных категориях и подтверждает, что Индекс НЕ является сбалансированным средством измерения. Данный факт отражается в снижении общего уровня вредоносной активности среди основной массы хостов.

Данная таблица показывает, почему каждый хост из представленного Топ 10 имеет столь высокий рейтинг.

Например, можно видеть, что AS47583 HOSTING-MEDIA получил место #1 по вредоносной активности главным образом из-за размещения там большого количества фишинговых, C&C и эксплоит-северов. При этом данный хост характеризуется низкой концентрацией сервисов Zeus, зараженных веб-сайтов и вредоносного программного обеспечения.

В тоже время AS16138 INTERIA.PL получил место # 6 только из-за большого количества угроз категории «Прочее».

Новое за квартал

7.1. Обзор

	Предыдущий квартал - Q3 2011			Текущий квартал - Q4 2011		
	Номер	Название АС	Страна АС	Номер	Название АС	Страна АС
#1	33626	Oversee.net	US	47583	Hosting Media	LT
#2	47583	Hosting Media	LT	33182	HostDime	US
#3	10297	eNET	US	10297	eNET	US
#1 Спам	45899	VNPT Corp	VN	55740	TATA Indicom	IN
#1 C&C-серверы	47583	Hosting Media	LT	47583	Hosting Media	LT
#1 Серверы Zeus	16125	Duomenu Centras	LT	16125	Duomenu Centras	LT
#1 Серверы фишинга	10297	eNET	US	45634	Sparkstation	SG
#1 Эксплойт серверы	47583	Hosting Media	LT	36444	Nexcess.net	US
#1 Вредоносное ПО	33626	Oversee.net	US	33626	Oversee.net	US
#1 Иные угрозы	33626	Oversee.net	US	25795	ARP Networks	US
#1 Иные угрозы	16138	Interia.pl	PL	16138	Interia.pl	PL

Исследование поквартальных тенденций указывает, насколько высоко хостинг-провайдеры оценивают критерий надежности хостинга.

Для ответственного хостера может быть настоящим шоком, когда он видит, что занимает высокие позиции в нашем списке или того хуже — оказывается на месте # 1. Этого может быть вполне достаточно для того, чтобы подтолкнуть его к срочным действиям по исправлению ситуации.

В качестве примера обратим внимание на самый плохой хост в III квартале 2011 года (он также получил место # 1 и в категории «Вредоносное ПО», и в категории «Зараженные веб-сайты») AS33626 Oversee.net. Этот клиентоориентированный поставщик услуг быстро выяснил причины столь нежелательного статуса. Реализация программы по очистке хоста от вредоносной деятельности и применение новых процедур позволило изменить ситуацию. (Более подробно об этом будет сказано в будущем исследовании.)

Очистка Oversee.net успешно продолжается, и мы уверены, что он сможет еще снизить свой рейтинг и покинуть место # 1 в категории «Вредоносное ПО».

7.2. Топ 10. Вновь зарегистрированные хосты

В конце IV квартала 2011 года в сети было обнаружено **39,796** автономных систем, что на **1,740** больше по сравнению с концом III квартала.

Ниже вы можете найти перечень 10 автономных систем, зарегистрированных в IV квартале 2011 года и обладающих наивысшим Индексом НЕ. Эти хосты представляют интерес в связи существенным уровнем вредоносной активности, зарегистрированным в короткий период времени.

Приведенный ниже список 10 автономных систем повторяет результаты двух предыдущих квартальных отчетов. В IV квартале была снова отмечена тенденция появления небольших, «одноразовых» хостов с малым сроком жизни, в то время как в III квартале были зарегистрированы две больших автономных системы на Тайване и одна в Китае.

Малые хосты, как правило, используются для быстрых атак типа «хватай и беги» («grab and run»).

	Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
2011 Q4	740	46.7	21508	COMCAST-21508 - Comcast Cable Communications Holdings, Inc	US	256
	1,356	34.0	4213	VPLSNET-EAST - VPLS Inc. d	US	2,048
	1,644	29.2	27626	AS-JOYTEL - Joytel	US	1,024
	1,986	25.2	57374	GIV-AS Commercial radio-broadcasting company Cable operator...	MK	7,168
	2,063	24.4	47311	ASBRESTRW Transport Republican unitary enterprise...	BY	256
	2,181	23.6	4.459	--No Registry Entry--	BR	256
	2,189	23.5	43463	BST-AS Biuro sprendimu tinklas UAB	LT	3,072
	2,406	21.9	57446	TELEMONT-AS Telemont Service S.R.L.	EU	4,096
	2,596	20.6	28015	MERCO COMUNICACIONES	AR	22,528
	2,905	18.7	3.961	ENERGOMONTAZH-AS ENERGOMONTAZH ltd.	EU	256
2011 Q3	57	98.1	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,920
	160	72.4	9929	CNCNET-CN China Netcom Corp.	CN	1,182,944
	269	64.6	33491	COMCAST-33491 - Comcast Cable Communications, Inc.	US	2,304
	333	61.4	9924	TFN-TW Taiwan Fixed Network, Telco and Network Service Provider.	TW	3,908,352
	364	60.6	7725	COMCAST-7725 - Comcast Cable Communications Holdings, Inc	US	1,536
	452	54.2	33668	CMCS - Comcast Cable Communications, Inc.	US	256
	460	53.9	9919	NCIC-TW New Century InfoComm Tech Co., Ltd.	TW	1,102,848
	542	50.6	33652	CMCS - Comcast Cable Communications, Inc.	US	1,024
	743	44.9	33489	COMCAST-33489 - Comcast Cable Communications, Inc.	US	0
	756	44.6	33490	COMCAST-33490 - Comcast Cable Communications, Inc.	US	1,024
2011 Q2	146	78.3	33651	CMCS - Comcast Cable Communications, Inc.	US	768
	179	73.5	33657	CMCS - Comcast Cable Communications, Inc.	US	256
	210	70.4	11380	INTERNETOFFICEPARKS	ZA	0
	295	60.6	49093	BIGNESS-GROUP-AS Bigness Group Ltd.	RU	512
	572	51.1	3.196	IM-AS Info-Media LTD	RU	256
	576	50.9	50073	SOFTNET Software Service Prague s.r.o.	CZ	256
	584	50.7	44088	DORINEX-AS SC Dorinex Pord SRL	RO	768
	768	45.7	42868	NIOBE Niobe Bilisim Backbone AS	US	4,096
	817	44.4	48671	ECSRV-AS Production United Enterprise Econom-Service Ltd	UA	256
	818	44.4	49798	SECUREHOST-NET-AS SecureHost LLC	RO	512

7.3. Вылеченные хосты

Изменение	Предыдущий квартал		Текущий квартал		Номер AC	Название AC	Страна AC	Количество IP
	Рейтинг	Индекс	Рейтинг	Индекс				
-88.8%	90	88.0	4,718	9.8	10922	LIVEJOURNAL - Live Journal Inc.	US	1,536
-68.8%	89	88.2	1,766	27.5	9512	NETLOGISTICS-AU-AP Net Logistics Pty. Ltd.	AU	13,568
-63.2%	33	111.6	1,012	41.1	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
-56.2%	41	106.8	738	46.7	29497	KUBANGSM CJSC Kuban-GSM	RU	22,784
-50.7%	1	292.7	12	144.2	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
-49.2%	51	101.0	590	51.3	39570	LOOPIA Loopia AB	SE	768
-49.2%	100	83.7	944	42.5	6400	Compañía Dominicana de Teléfonos	DO	456,448
-48.7%	45	105.0	524	53.8	8661	PTK PTK IP	RS	97,280
-46.6%	103	83.3	845	44.5	13174	MTSNET OJSC "Mobile TeleSystems"	RU	24,320
-46.3%	38	108.8	435	58.5	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512

Хосты, указанные в таблице выше, все без исключения продемонстрировали значительное снижение содержания нежелательного контента за три месяца, прошедшие с момента выпуска отчета за III квартал 2011 года.

Многие виды вредоносного кода могут причудливо взаимодействовать друг с другом, представляя собой систему, которую провайдеры практически не могут отследить самостоятельно. Однако мы с радостью поддерживаем усилия этих 10 хостов, улучшивших свои позиции в рейтинге. Они сильно отличаются друг от друга размером, местом расположения, видом бизнеса и категориями вредоносного контента, с которыми им удалось справиться. Они доказывают, что снижение уровня присутствия вредоносного программного обеспечения возможно в любых обстоятельствах. Нужно лишь приложить некоторые дополнительные усилия и думать нестандартно.

Улучшения, заслуживающие внимания:

AS10922 Live Journal Inc. переместился вниз с позиции # 90 до # 4718, снижение вредоносной активности составило 88,8 %.

AS33626 Oversee.net улучшил свою позицию в рейтинге на 98,5 % процентов, снизив содержание вредоносного контента до ничтожно малого уровня.

7.4. Хосты, состояние которых ухудшилось

Изменение	Предыдущий квартал		Текущий квартал		Номер AC	Название AC	Страна AC	Количество IP
	Рейтинг	Индекс	Рейтинг	Индекс				
837.2%	3,808	12.2	33	114.5	25795	ARPNET - ARP NETWORKS, INC.	US	12,288
619.3%	3,368	14.8	46	106.5	40034	CONFLUENCE-NETWORK-INC - Confluence Net...	VG	3,328
535.3%	3,440	14.3	79	91.0	50465	IQHOST IQHost Ltd	RU	3,584
301.6%	842	42.5	4	170.8	45634	SPARKSTATION-SG-AP 10 Science Park Road	SG	3,072
176.1%	1,067	38.1	49	105.2	12260	COLOSTORE - Colostore.com	US	53,248
153.2%	620	48.5	26	122.9	36444	NEXCESS-NET - NEXCESS.NET L.L.C.	US	115,968
80.5%	189	69.7	22	125.8	45538	ODS-AS-VN Online data services	VN	9,472
75.2%	438	55.1	66	96.5	18866	ATJEU - atjeu publishing, llc	US	13,312
71.4%	501	52.4	80	89.8	18059	DTPNET-AS-AP DTPNET NAP	ID	16,128
59.1%	517	51.6	109	82.2	38676	AS33005-AS-KR wizsolution co.,Ltd	KR	10,528

Перечисленные хосты продемонстрировали наибольший рост уровня вредоносного контента в прошедшем квартале. Для них мы рекомендуем пересмотреть недавно произведенные изменения, которые могли вызвать неожиданный подъем уровня вредоносной активности. Информация по вновь зарегистрированным хостам отражена в разделе 7.2.

Самым «выдающимся» хостом в этом квартале стал AS25795 Arp Networks, значительно увеличивший уровень присутствия вредоносного контента. Прежде снижавший свой рейтинг ArpNetworks недавно перескочил на позицию # 33 по общему уровню активности киберпреступников. Arp Networks занимает место # 1 в категории «Зараженные веб-сайты».

Второе место по ухудшению состояния занял хост AS40034 Confluence Network Inc. Confluence Network занял высокие позиции (место # 4) за размещение серверов C&C, а также ботнетов Zeus (место # 6). Теперь Confluence Network переместился на место # 46 в общем рейтинге, хотя демонстрировал низкий уровень вредоносной активности в начале 2011 года.

AS45634 Sparkstation SG-AP также уверенно поднимает вверх по рейтингу. В третьем квартале Sparkstation занимал место # 842, а теперь перебрался на позицию # 4 в общей таблице. Также Sparkstation занимает # 1 место в категории «Фишинговые серверы»» и место # 6 в категории «Вредоносное ПО».

Анализ по странам

Как было отмечено в предыдущих отчетах, мы работаем над методикой более точного определения уровня вредоносной активности, представленного в автономных системах в каждой отдельной стране. С этим процессом связан ряд трудностей, таких как невозможность точного определения физического местонахождения сервера в автоматическом режиме.

Однако при тщательном подходе возможно получить вполне достоверные данные.

Ранее мы перечислили «худшие» страны, просто сложив количество хостов, взятых из Топ 50 и Топ 250, для отдельной страны. Этот подход исказил результаты для стран, имеющих большое количество хостов, что противоречит философии нашего отчета, целью которого является предоставление данных о концентрации вредоносного контента.

Что же мы сделали иначе в этот раз? Теперь мы рассматриваем каждую страну как индивидуальную автономную систему, суммируя количество IP-адресов и случаев вредоносной активности во всех автономных системах, зарегистрированных в этой стране. Затем мы рассчитываем индекс для каждой страны, используя ту же методику как для отдельных хостов.

В результате «Индекс страны», оценивающий уровень вредоносной активности в стране, определяемый по шкале из 1000 единиц, практически не зависит от количества хостов в этой стране.

В таблице перечислены Топ 10 стран, определенные согласно этой методике:

Данные о стране				Оценка	
Код	**Название**	**Количество АС**	**Общее количество IP**	**Рейтинг**	**Индекс**
LV	LATVIA	189	1,690,880	1	237.66
VG	VIRGIN ISLANDS, BRITISH	3	7,680	2	235.72
LU	LUXEMBOURG	42	1,106,432	3	213.84
MD	MOLDOVA, REPUBLIC OF	32	1,075,648	4	213.70
US	UNITED STATES	13,823	1,253,081,312	5	194.00
LT	LITHUANIA	94	2,463,744	6	182.97
CZ	CZECH REPUBLIC	820	7,887,872	7	177.33
NL	NETHERLANDS	427	17,189,568	8	171.73
RU	RUSSIAN FEDERATION	3,188	45,432,640	9	171.43
BY	BELARUS	68	1,667,328	10	169.60

Результаты принципиально отличаются от предыдущих отчетов. Наиболее ярко это можно видеть по появлению в рейтинге Виргинских островов, занимающих место # 2. Таким образом, при вычислении индекса теперь учитывается «размер» страны (количество зарегистрированных автономных систем) и, следовательно, определяется концентрация вредоносной активности.

В следующем отчете, который будет опубликован в феврале, мы подробнее рассмотрим использование этой методики. Более того, в нем будут реализованы дальнейшие изменения, позволяющие дополнительно повысить точность результатов (включая улучшенное определение реального местоположения хоста).

«Чистые» хосты

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
37,296	0.57	721	DNIC-ASBLK-00721-00726 - DoD Network Information Center	US	90,705,408
36,682	0.68	6203	ISDN-NET - The Nexus Group, Inc.	US	185,856
36,506	0.70	21976	NJEDGE-NET - NJEDge.Net, Inc.	US	150,080
36,359	0.71	14985	VEROXITY - Veroxity Technology Partners, Inc.	US	133,632
35,565	0.73	17645	NTT-SG-AP ASN - NTT SINGAPORE PTE LTD	SG	115,200
11,120	1.14	378	MACHBA-AS ILAN	EU	1,160,192
11,047	1.21	50915	ASEVERHOST S.C. Everhost S.R.L.	RO	222,208
9,666	1.70	71	HP-INTERNET-AS Hewlett-Packard Company	US	35,047,424
9,547	1.87	10970	LIGHTEDGE - LightEdge Solutions	US	103,680
9,373	2.06	17229	ATT-CERFNET-BLOCK - AT&T Enhanced Network Services	US	83,712

9.1. Для чего нужна таблица «чистых» хостов?

Было бы некорректно отметить только поставщиков услуг, содержащих зараженные хосты. Для полноценности отчета мы выделили 10 организаций с минимальным уровнем нарушений. Обеспечение безопасного хостинга вебсайтов вполне посильная задача и данные 10 компаний явный тому пример.

Компании, представленные в нашей таблице «чистых» хостов, являются образцом для подражания, и мы бы хотели поблагодарить их за борьбу со злонамеренной деятельностью в подконтрольной им сфере.

Данные раздел является постоянной частью нашего отчета.

9.2. Критерии отбора

Мы отбираем «чистые» хосты среди интернет-провайдеров, хостинг провайдеров или организаций, которые владеют минимум 10000 выделенными IP-адресами. Многие хостинг-провайдеры, представленные в других разделах данного отче та, обладают меньшим количеством адресов. Тем не менее, в данном разделе наше исследование фокусируется в основном на крупных провайдерах, которые должны иметь достаточное количество ресурсов для обеспечения полного диапазона профилактических услуг, включая 24-часовую поддержку клиентов, сетевой мониторинг и высокий уровень технической квалификации.

Мы также включали только публичные автономные системы и автономные системы интернет-провайдеров, хотя мы понимаем, что такая оценка является субъективной.

Опасные хосты по категориям

10.1.1. C&C-серверы

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**953.29**
30	120.41	**40824**	WZCOM-US - WZ Communications Inc.	**US**	9,216	**611.92**
135	76.43	**36408**	ASN-PANTHER Panther Express	**US**	79,616	**429.23**
46	106.48	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	3,328	**359.34**
16	132.40	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**275.95**
226	68.74	**37963**	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co., Ltd.	**CN**	828,416	**236.82**
27	121.97	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,571,072	**200.35**
263	65.31	**39134**	SKYMEDIA United Network LLC	**RU**	16,384	**185.87**
8	148.70	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	235,776	**179.14**
68	95.16	**27715**	LocaWeb Ltda	**BR**	107,264	**178.42**

Категория «Серверы управления ботнетами» показывает распределение данного вида угроз в сетях различных провайдеров. Наши собственные данные в данном случае объединены с информацией, предоставленной Shadowserver.

Позиция США стабильно улучшается от отчета к отчету, и теперь по итогам IV квартала. В этот раз США представлена 3 позициями в списке Топ 10 худших хостов по размещению серверов управления ботнетами

10.1.2. Серверы фишинга

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
4	170.85	**45634**	SPARKSTATION-SG-AP 10 Science Park Road	**SG**	3,072	**926.10**
3	181.18	**10297**	ENET-2 - eNET Inc.	**US**	90,624	**839.45**
40	111.87	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,704	**769.13**
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**727.92**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**678.36**
63	98.88	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816	**497.79**
22	125.82	**45538**	ODS-AS-VN Online data services	**VN**	9,472	**426.28**
17	132.15	**24971**	MASTER-AS Master Internet s.r.o	**CZ**	43,520	**416.67**
5	162.79	**32475**	SINGLEHOP-INC - SingleHop	**US**	248,064	**416.45**
8	148.70	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	235,776	**394.73**

Фишинг и социальная инженерия остаются основными источниками проблем для банков и корпораций всех размеров.

Примечательно, что каждый из хостов, занимающих позиции от пятой и выше в общей таблице рейтинга Топ 50, обязательно представлен и в списке Топ 10 в категории «Серверы фишинга».

И только один из хостов, попавших в Топ 10 в данной категории, не входит в общий рейтинг Топ 50.

10.1.3. Эксплойт серверы

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
26	122.93	**36444**	NEXCESS-NET - NEXCESS.NET L.L.C.	**US**	115,968	**1,000.00**
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**557.03**
34	114.12	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	11,264	**472.92**
109	82.18	**38676**	AS33005-AS-KR wizsolution co.,Ltd	**KR**	10,528	**405.35**
772	45.99	**17185**	QUONIXNET - Quonix Networks Inc.	**US**	15,872	**361.10**
309	62.51	**50673**	SERVERIUS-AS Serverius Holding B.V.	**NL**	14,848	**234.30**
358	60.41	**8455**	ATOM86-AS ATOM86 Autonomous System	**NL**	17,152	**226.23**
704	47.64	**13332**	SVWH - Silicon Valley Web Hosting, Inc.	**US**	40,192	**219.24**
3,241	16.86	**57297**	GENIUS-AS Genius Investments (Cyprus) Limited	**RU**	256	**214.10**
1,444	32.43	**51331**	YOURNAME Your Name Webhosting	**NL**	768	**211.34**

Мы считаем категорию «Эксплойт-серверы» наиболее важной при анализе вредоносного ПО, фишинга и вредоносной активности в целом. Поэтому данному сектору был придан дополнительный вес. Вы можете более подробно ознакомиться с методикой оценки в приложении 2.

Хосты и корпоративные серверы могут распространять вредоносное ПО или выполнять другие злонамеренные действия в результате взлома или компрометации. Важная информация, персональные данные жертв и другие данные, полученные нелегальным путем, направляются на эксплойт-серверы при помощи вредоносного ПО.

Четыре хоста, из представленных в Топ 10 в прошлом отчете, также присутствуют и в нынешнем. Эти хосты должны немедленно обратить внимание на данный факт, так как их репутация уже значительно пострадала.

Позиция # 1 в этой категории — AS36444 Nexcess. Ранее он демонстрировал низкий уровень вредоносной активности. Это указывает на тот факт, что данный хост был скомпрометирован или взломан.

10.1.4. Серверы Zeus

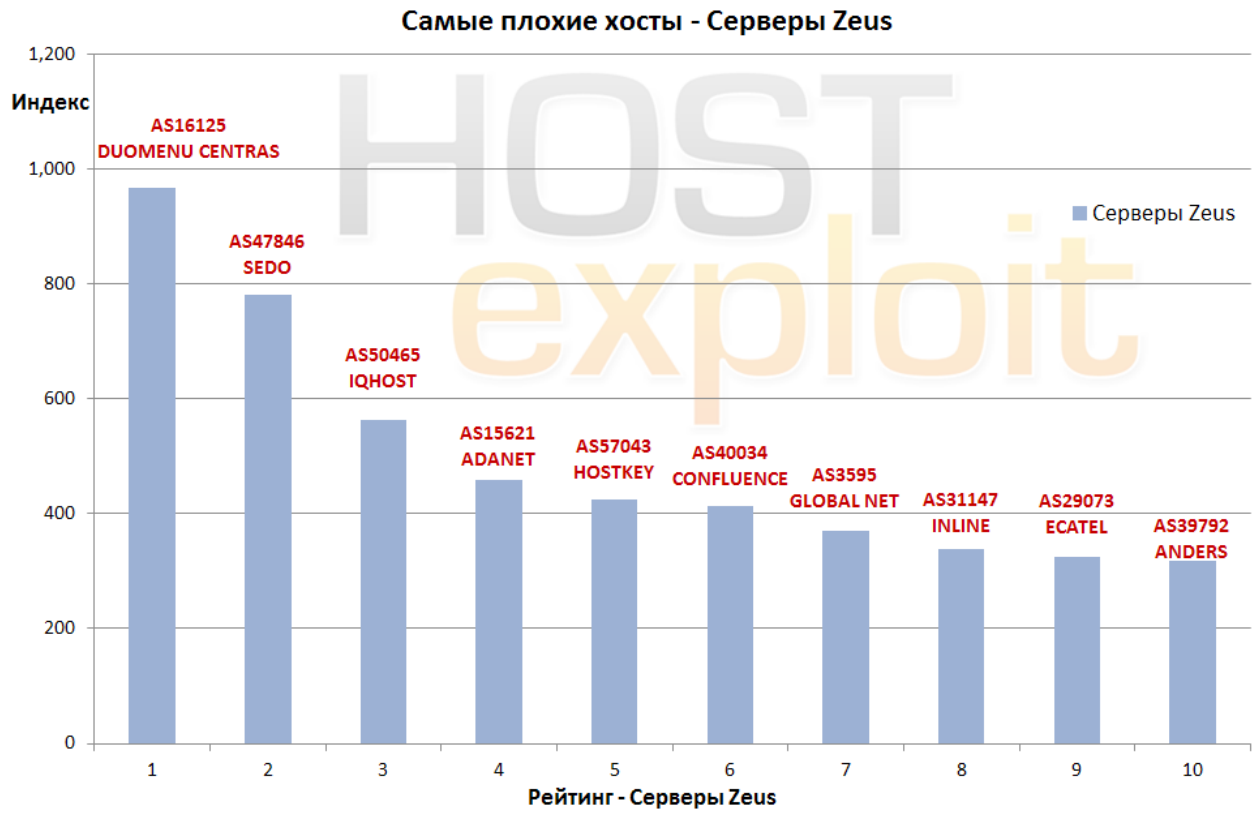
Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
44	108.20	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**966.70**
39	112.63	**47846**	SEDO-AS Sedo GmbH	**DE**	1,280	**780.53**
79	91.04	**50465**	IQHOST IQHost Ltd	**RU**	3,584	**563.84**
103	83.74	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	11,264	**458.09**
678	48.20	**57043**	HOSTKEY-AS HOSTKEY B.V.	**NL**	2,304	**425.76**
46	106.48	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	3,328	**412.43**
7	152.61	**3595**	GNAXNET-AS - Global Net Access, LLC	**US**	159,232	**369.89**
34	114.12	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	11,264	**338.77**
9	146.10	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**323.91**
186	71.68	**39792**	ANDERS-AS Anders Telecom Ltd.	**RU**	35,072	**317.70**

Киберпреступники управляют сетями инфицированных компьютеров, известных также как «зомби», отделяя сам ботнет от серверов управления. Один C&C сервер может управлять более чем 250 000 зараженных компьютеров. При этом Zeus-ботнет остается наиболее дешевым и популярным ботнетом на черном рынке.

Этот раздел следует рассматривать совместно с разделом 10.1.3, посвященным эксплойт-серверам.

Приведенный список часто содержит имена хостов, хорошо известных обозревателям и исследователям киберпреступности, некоторые из уже были уличены в неправомерных действиях.

Данные, полученные от abuse.ch, известного ресурса, исследующего Zeus, использованы вместе с собственными данными НЕ.



10.2.1. Зараженные веб-сайты

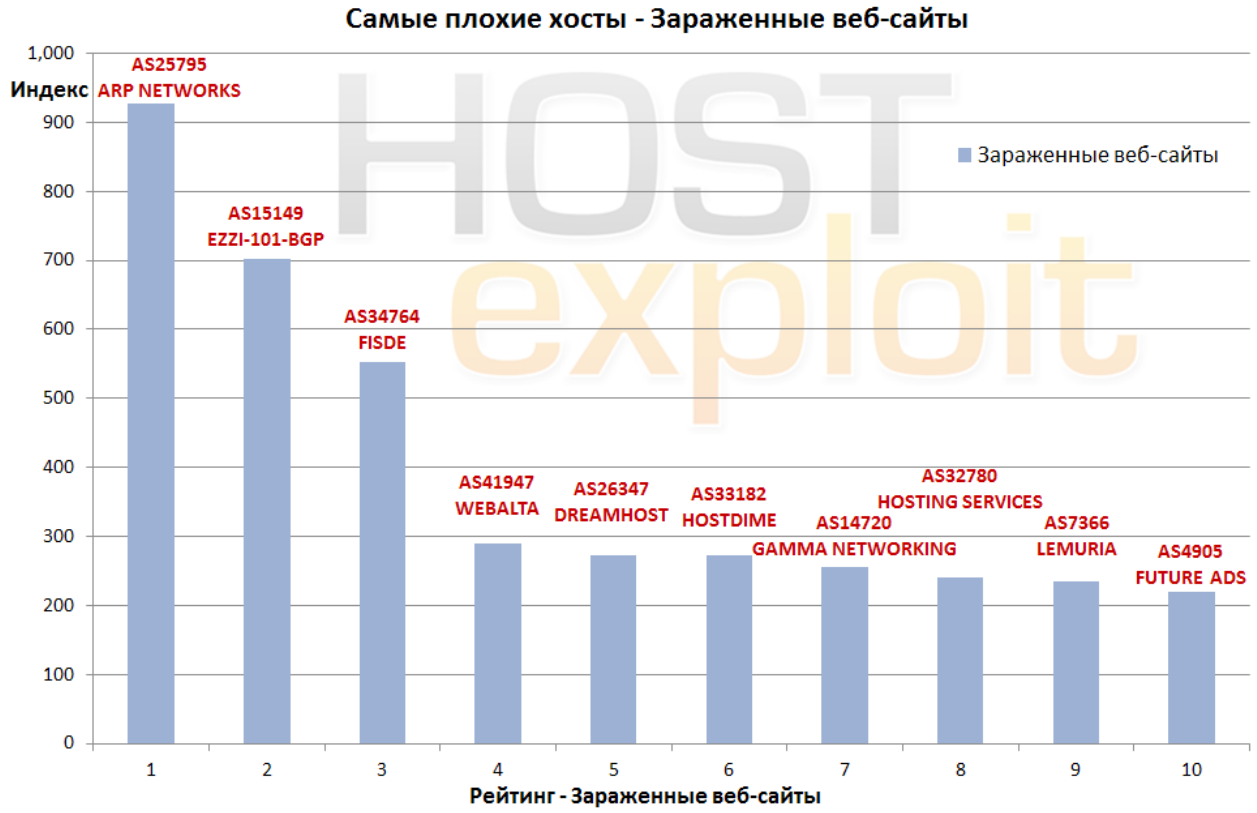
Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
33	114.46	**25795**	ARPNET - ARP NETWORKS, INC.	**US**	12,288	**927.26**
25	124.92	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,928	**702.01**
315	62.22	**34764**	FISDE-AS Maurice Funke	**DE**	1,280	**551.73**
28	121.32	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,872	**289.29**
15	132.81	**26347**	DREAMHOST-AS - New Dream Network, LLC	**US**	329,216	**272.73**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**272.53**
207	70.52	**14720**	GAMMANETWORKING-EAST - Gamma Networking Inc.	**CA**	7,680	**255.52**
108	82.88	**32780**	HOSTINGSERVICES-INC - Hosting Services, Inc.	**US**	12,288	**241.22**
794	45.55	**7366**	LEMURIACO - Lemuria Communications Inc.	**US**	3,072	**235.33**
1,964	25.34	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**219.37**

«Зараженные веб-сайты» — это обширная категория ресурсов, где могут сосуществовать несколько видов угроз. Интернет-ресурсы могут намеренно размещать вредоносный контент или быть скомпрометированными.

В этом разделе данные нашего собственного исследования, собранные из различных ловушек, объединены с данными Clean-MX и hphosts относительно количества вредоносных URL, обнаруженных в отдельных автономных системах.

Результаты исследования отражают деятельность больших хостов, а также менее масштабных, подозреваемых в криминальных действиях.

Примечательно, что целый кластер хостов из США оказался в этой категории.

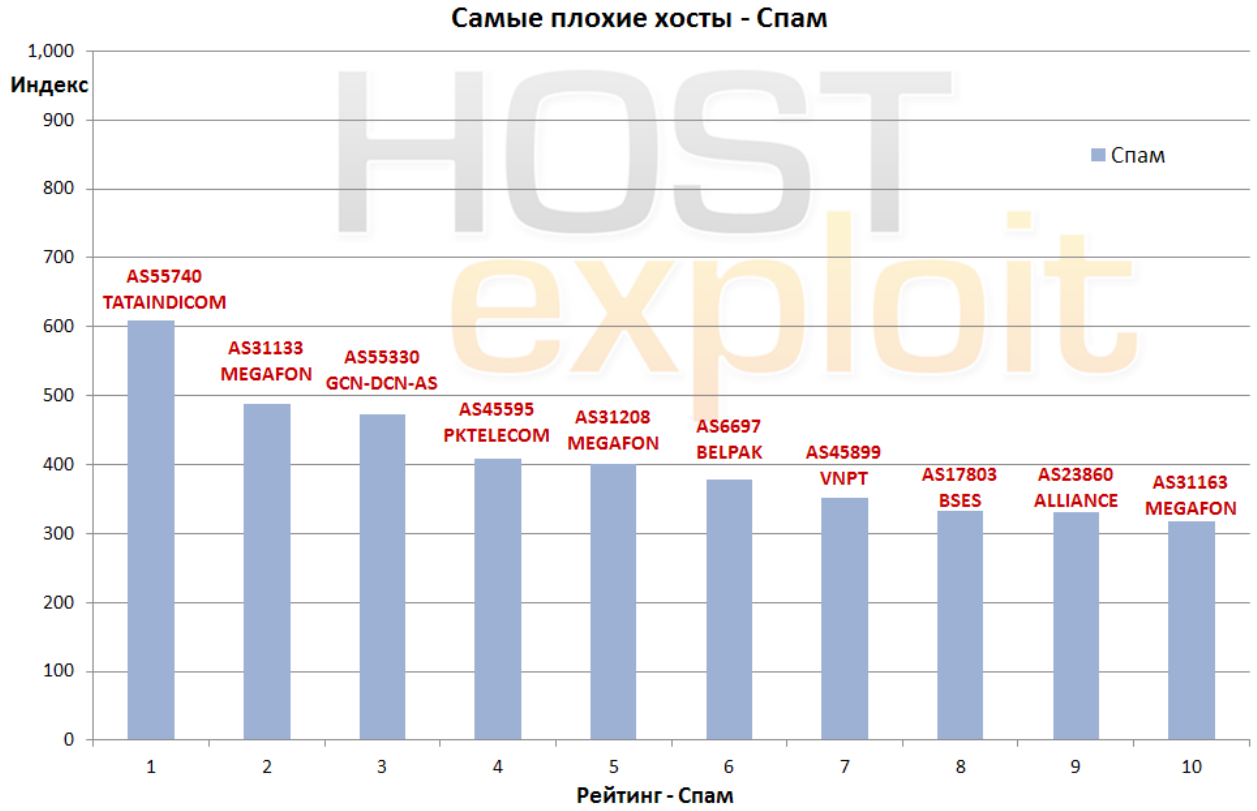


10.2.2. Спам

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
14	135.54	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM	**IN**	259,072	**609.86**
32	119.64	**31133**	MF-MGSM-AS OJSC MegaFon	**RU**	19,456	**487.29**
50	105.03	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUN...	**AF**	16,384	**472.08**
71	94.56	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,824,384	**408.80**
85	89.48	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	4,096	**401.84**
23	125.35	**6697**	BELPAK-AS Republican Association BELTELECOM	**BY**	1,074,432	**377.65**
57	100.30	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,220,288	**351.93**
114	81.38	**17803**	BSES-AS-AP BSES TeleCom Limited	**IN**	1,034,752	**332.76**
154	73.71	**23860**	ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services...	**IN**	17,408	**331.20**
200	70.93	**31163**	MF-KAVKAZ-AS JSC MegaFon	**RU**	5,120	**318.40**

Список Top 10 по категории спама отражает расположение серверов, наиболее активно используемых для рассылки нежелательных писем. Страны с минимальным регулированием в этой сфере и недостаточным мониторингом позволяют спамерам использовать старые проверенные методы, позволяющие избежать детектирования, такие как серверы fast-flux и одноразовые северы. В дополнение к этому злоумышленники быстро адаптируются к актуальным темам СМИ, что не требует поиска новых методик, как в других областях деятельности киберпреступности.

Один спам-сервер может нанести такой же урон, как целая группа серверов, рассылающих нежелательные письма. Более того, небольшое количество спама может быть более эффективно, чем массовая рассылка, если исполнитель применяет специальные технологии адресной выборки получателей. Эти две особенности делают затруднительной количественную оценку в данной категории. Поэтому мы совместили данные об IP-адресах, с которых происходит рассылка спама, принимая во внимание широкий спектр авторитеных источников – SpamHaus, UCEPROTECT-Network, Malicious Networks (FiRE) и SudoSecure – а также наши собственные данные. В результате получился достаточно точный и актуальный список спам-серверов по всему миру, то есть серверов, с IP-адресов которых происходит отправка спама.



10.2.3. Иные угрозы

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
6	160.09	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**949.48**
43	108.43	**15169**	GOOGLE - Google Inc.	**US**	281,344	**329.30**
446	57.72	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.73**
9	146.10	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.08**
25	124.92	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,928	**185.74**
540	52.94	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.32**
18	129.29	**21788**	NOC - Network Operations Center Inc.	**US**	281,088	**178.62**
2,822	19.25	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	256	**164.28**
27	121.97	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,571,072	**157.68**
236	67.72	**29131**	RAPIDSWITCH-AS RapidSwitch	**GB**	0	**152.32**

Наиболее актуальные и меняющиеся виды и векторы атак содержатся в категории «Прочие угрозы».

Здесь приведены различные виды активности, включая MALfi (XSS/RCE/RFI/LFI), XSS-атаки, скликивание, черный фарм-бизнес, поддельные антивирусы, Zeus (Zbota), Artro, SpyEye, Stuxnet, черный SEO, Koobface и новые вредоносные инструменты.

Широкий спектр техник, рассматриваемых в данной категории, отражен в рейтинге Топ 10 «Прочие угрозы», в который попали несколько хорошо известных имен.

Также, как и в III квартале, 40% из Топ 10 находятся в США.

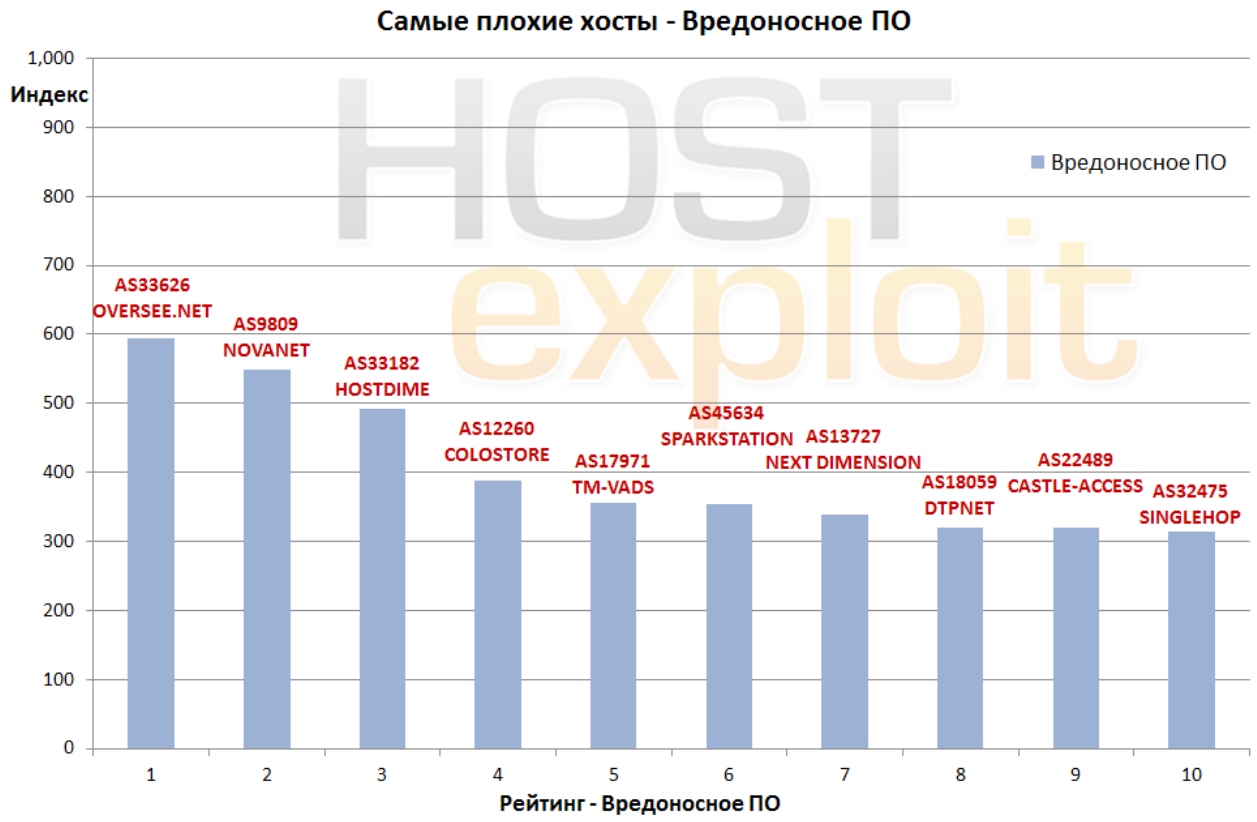
10.2.4. Вредоносное ПО

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
12	144.19	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**594.37**
41	111.18	**9809**	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	**CN**	10,496	**548.46**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**491.96**
49	105.23	**12260**	COLOSTORE - Colostore.com	**US**	53,248	**387.48**
35	114.07	**17971**	TMVADS-AP TM-VADS Datacenter Management	**MY**	40,320	**355.31**
4	170.85	**45634**	SPARKSTATION-SG-AP 10 Science Park Road	**SG**	3,072	**353.87**
81	89.82	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**337.88**
80	89.82	**18059**	DTPNET-AS-AP DTPNET NAP	**ID**	16,128	**320.58**
16	132.40	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**319.03**
5	162.79	**32475**	SINGLEHOP-INC - SingleHop	**US**	248,064	**313.30**

Вредоносное ПО использует зараженные компьютеры в своих целях. В качестве примеров можно рассмотреть шпионские программы, вирусы, поддельные программы и назойливую рекламу. Обычно такое ПО распространяется в качестве бесплатных заставок для рабочего стола, которые постоянно выдают рекламу, направляют браузер на неожиданные страницы, а также загружают кейлоггеры, пересылающие персональные данные злоумышленникам.

В этом квартале был произведен более глубокий анализ «ложного детектирования», в частности относительно запаркованных доменов. В их отношении было выявлено некоторое количество несоответствий, и мы продолжаем работать с ответственными хостами, чтобы улучшить методологию анализа в данной области.

Результаты исследования в категории были основаны главным образом на данных Google, Sunbelt Software, и Team Cymru.



Выводы

В этом квартале самый плохой хост был обнаружен не в США, а в Латвии. Действия этого провайдера были таковы, что многие исследователи не удивятся тому, что он занял данную позицию. AS47583 Hosting Media поддерживает некоторые из наиболее вредоносных типов угроз, включая несколько ботнетов, таких как Zeus, а также серверы C&C, эксплойт-серверы, фишинг-серверы и различное вредоносное ПО. Мы надеемся, что выдвижение данного провайдера на первый план поможет ему улучшить ситуацию, как и другими хостами, которые прежде занимали позицию # 1.

Среди хостов, улучшивших свое положение, следует отметить AS33626 Oversee.net, который в настоящее время продолжает отслеживать вредоносную активность в собственных сетях, что позволяет надеяться на дальнейшее снижение его позиций в рейтинге.

Среди хостов, которые требуют пристального внимания, следует выделить AS45634 Sparkstation, поднявшийся до места # 4, который до этого месяцами находился в низу списка Топ 1000. Теперь же хостинговая компания, расположенная в Научном Парке Сингапура, выделяется широким спектром вредоносной активности.

Итак, 2011 закончился с теми же тенденциями, что и начинался, поэтому многие называют его «годом взлома систем безопасности» или даже годом хаоса, который сопровождался многочисленными взломами и публикацией персональных данных в Сети. Также следует констатировать рост количества видов вредоносного ПО для смартфонов, в частности для платформы Android, ставшей наиболее часто атакуемой. Потенциально мы находимся на пороге появления первых крупных мобильных ботнет, в то время пока разработчики мобильных решений продолжают играть в «догонялки», что напоминает ранние этапы зарождения вирусов для настольных ПК.

По мере того, как тенденция «Используй свои личные устройства» (BYOD) набирает обороты, работодателей ждет сложный год. Крупные организации, как мы надеемся, смогут ответить данному вызову, но меньшие компании продолжают балансировать между потребностями в безопасности и сокращении издержек.

Обновленная методология составления рейтинга по странам дала интересные результаты, которые получат дальнейшее развитие в февральском отчете.

Заканчивая на более позитивной ноте, отметим, что 2012 год может дать новые результаты благодаря международному взаимодействию, но только если страны объединят свои усилия в борьбе с общим врагом. Ведь ни одна страна не выигрывает, когда ее экономика постоянно страдает от вредоносной активности киберпреступников, атакующих из-за границы. Итак, мы обращаемся ко всем: «Объединяйтесь и работайте вместе, чтобы принести процветание всем нам».

Все участники HostExploit и члены нашего сообщества желают вам счастливого нового 2012 года!

Джарт Армин

(Jart Armin)

Приложение 1

Словарь

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.

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 HE — значение от 0 (зараженность отсутствует) до 1000 (максимальный уровень зараженности). Желаемые свойства Индекса HE 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 HE 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 HE 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.	StopBadware	Образцы вредоносного ПО	Очень высокая
4.	SudoSecure	Спам-боты	Средняя
5.	Malicious Networks	Командные и управляющие сервера	Высокая
6.	Malicious Networks	Сервера фишинга	Средняя
7.	Malicious Networks	Сервера с эксплойтами	Средняя
8.	Malicious Networks	Сервера для рассылки спама	Низкая
9.	«HostExploit»	Текущие события	Высокая
10.	hpHosts	Образца вредоносного ПО	Высокая
11.	Clean MX	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.

Информация, полученная с ресурса StopBadware, сама по себе является сочетанием данных от корпораций Google, Sunbelt Sofware и NSFOCUS.

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:

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

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:

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

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:

$$F_A = min\{\frac{N}{N_a}, 1\} \tag{3}$$

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:

$$F_B = \frac{N}{N_m - N_a} \tag{4}$$

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 HE до 1,000, как указано в заданном свойстве № 4.

Индекс для каждого источника данных может быть рассчитан следующим образом:

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

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 HE-индекс далее рассчитывается как:

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

где:

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