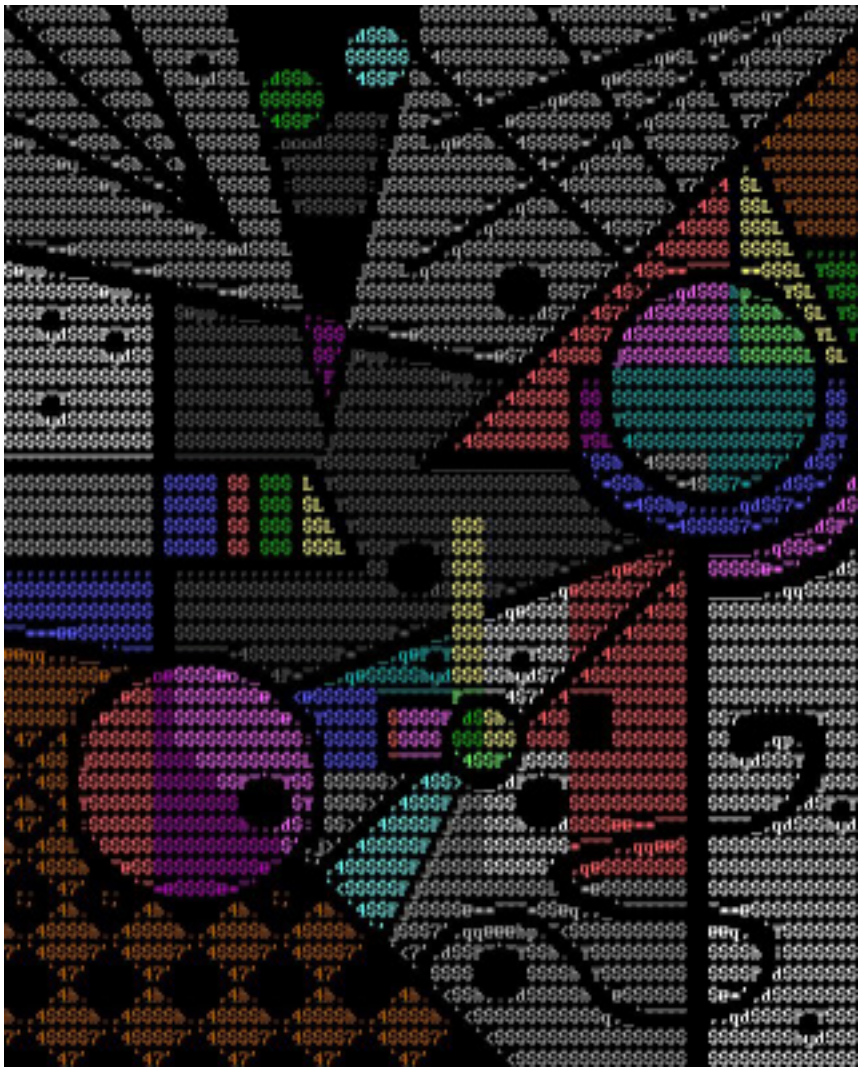
HostExploit Всемирный обзор кибепреступлений

Топ 50 «Самые плохие сети и хосты»

Отчет по итогам третьего квартала 2011 года



SITEVET HOST exploit GROUP IB

Оглавление

	Обзор текущих событий	4
1.	Введение	7
2.	Часто задаваемые вопросы	8
3.	Топ 50	9
4.	Сравнение второго и третьего квартала 2011 года	10
5.	График распределения Индекса НЕ	11
6.	Новое за квартал	12
	6.1 Обзор	12
	6.2 Вновь зарегистрированные хосты	13
	6.3 Вылеченные хосты	14
	6.4 Хосты, состояние которых ухудшилось	15
7.	Анализ по странам	16
8.	«Чистые» хосты	17
9.	Опасные хосты по категориям	18
	9.1 Серверы	
	9.1.1 Серверы управления ботнетами	18
	9.1.2 Серверы фишинга	19
	9.1.3 Эксплойт-серверы	20
	9.1.4 Серверы Zeus	21
	9.2 Направления деятельности	
	9.2.1 Зараженные веб-сайты	22
	9.2.2 Спам	23
	9.2.3 Иные угрозы	24
	9.2.4 Вредоносное ПО	25
10.	Выводы	26
Приложение 1	Словарь	27
Приложение 2	Методология	30

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
- Ilya Sachkov
- Alexander Pisemskiy

Авторы

- Philip Stranger
- James McQuaid
- Steve Burn
- David Glosser
- Greg Freezel
- Brynd Thompson
- Will Rogofsky

Использованные источники

- AA419
- Abuse.CH
- CIDR
- Clean-MX.DE
- Emerging Threats
- Google Safebrowsing
- 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: Juio Sepia - Kandinskii - ASCII art - http://www.juliosepia.com/2010/portafolio/kandinskii/lang/en

Самые плохие сети и хосты

DigiNotar и безопасность центров сертификации

Одним из наиболее интересных фактов, связанных с взломом голландской компании DigiNotar, выпускающей цифровые сертификаты, является общее мнение о том, что данное хищение было проведено для перехвата передач цифровой информации в Иране. Впрочем, некоторые недавно полученные доказательства противоречат данной точке зрения.

Данная история все больше напоминает уже ставшую классической ситуацию, когда компания очень медленно реагирует на серьезную атаку компьютерных злоумышленников. Возможно, «метания во тьме» — это слишком сильная характеристика того, как DigiNotar справлялась с этим взломом. Но в лучшем случае инцидент показал несовершенство защиты центров сертификации. В худшем — он свидетельствует о самом крахе системы центров сертификации и доверия сторонним компаниям.

Большинство новостей в этом квартале касаются выдаче поддельных сертификатов Google для доступа к Gmail. По сообщениям правительства Нидерландов был обнаружен 531 фальсифицированный сертификат, что нашло отражение в оперативно опубликованном предварительном отчете. Также следует отметить обнаруженные фальшивые сертификаты для следующих ресурсов: URL из зон .com или .org; браузеров Microsoft и Mozilla; движках Twitter, Wordpress, Equifax и Torproject (для анонимного просмотра узлов Tor); приложений Android; Facebook; и государственных ресурсов особой важности — CIA.gov и sis.gov.uk (MI6).

Голландская компания Fox-IT, занимающаяся информационной безопасностью и нанятая правительством для подготовки отчета, отметила, что после взлома было зарегистрировано 300,000 уникальных IP-адресов, с которых делались запросы на Google.com с использованием фальшивого сертификата Google. Сам сертификат был обнаружен в Иране. Около 1% запросов поступало через прокси-сервер Tor, находящийся за пределами Ирана. В отчете сообщается, что целью взлома мог быть перехват частных сообщений иранских интернет-пользователей.

Издатель сертификатов DigiNotar BV был приобретен Vasco Data Security International Inc. за $12,9 миллионов в январе 2011 года. Взлом был совершен 6 июня 2011 года (если не раньше), а обнаружен — лишь 19 июля. DigiNotar BV предоставляет цифровые сертификаты, включая SSL (Secure Sockets Layer), проверенные сертификаты и сертификаты голландского правительства, нескольким центрам сертификации.

Хакер(ы) использовал разные учетные записи и, похоже, оставил сообщения для Anonymus и LulzSec. Немного веселая вводная часть сообщения хакера на PasteBin — "Снова привет! Я снова атакую, ага?" — противоречит очевидной и пугающей причине атаки. Называющий себя ICHSUN (@ICHSUN2 на Twitter) иранский хакер, взломавший систему безопасности центров сертификации Comodo в марте 2011, сообщает, что это была месть за выдачу мусульманских солдат голландским правительством, которые впоследствии были жестоко убиты сербскими повстанцами во время беспорядков в стране 16 лет назад.

Fox-IT подтверждает, что сигнатуры кода совпадают с обнаруженными при взломе системы сертификации Comodo хакером ICHSUN в марте, когда также были созданы поддельные сертификаты. Другие идентификационные признаки были удалены. С одной стороны, навыки хакера(ов) были оценены как «любительские» , но, с другой стороны, по некоторым пунктам он(и) получил очень высокие оценки.

Сегодня можно выделить три вероятных гипотез, связанных с атакой на DigiNotar:

- Хакер-одиночка, использующий ник ICHSUN, действительно существует. Именно он опубликовал администраторские логины и пароли из DigiNotar и описал, как самостоятельно работать с библиотекой XUDA (Xcert Universal Database API), которая используется при выдаче сертификатов различными вендорами, в том числе RSA Security Inc. (Nasdaq: EMC).
- Обнаружение фальшивых сертификатов Google только на иранских прокси-серверах позволяет предположить возможность перехвата зашифрованной переписки со стороны иранских властей.
- Конечно, это может быть такой же, как Stuxnet, "черной цифровой операцией" против Ирана, которая должна была создать определенный цифровой беспорядок. Интересно, что Stuxnet также использовал поддельные сертификаты против Ирана.

Как бы ни обстояли дела, очевидно, что сегодня необходимо найти альтернативу центрам сертификации. "Доверенные" сертификаты больше не соответствуют своему описанию. Как отметил Рик Фергюсон из Trend Micro: "Можно ли сказать, что данное событие разрушает всю систему безопасных коммуникаций? Нет, конечно. Но оно определенно выявляет слабое звено в данной цепи".

Данная атака, Stuxnet и прочие взломы говорят о грядущих атаках с использованием ресурсов доверенных сторонних компаний и поддельных сертификатов. Таким образом, всему сообществу нужно найти новый и более безопасный способ шифрования данных и сертификации.

Shady Rat: выводы

- **Продолжительность проникновения, подтвержденная протоколами.** Просматривая log-файлы, мы часто видим, что похожие взломы остаются необнаруженными месяцы и даже годы, несмотря на то, что некоторые эксперты горячо доказывают, что ни один хакер не может сохранить доступ к серверу так долго. В случае с Shady RAT и 72 целями, средняя продолжительность работы хакера на ресурсе составляла 8.74 месяца.
- **APT-атаки – это не только PR-шумиха.** Shady RAT помогает определить назначение и природу APT-атак.
- **Жажда секретов и интеллектуальной собственности.** Специалисты McAfee не охарактеризовали этот инцидент как киберпреступление, т.к. считают этот термин более серьезным и конкретным. Однако дебаты о том, была ли Shady RAT результатом работы правительства или коммерческим заказом не прекращаются. Учитывая, что подобная атака была проведена на множество похожих торговых марок за последние десять лет, все же разумно считать данные инциденты результатами действий киберпреступности.
- **Это не новая атака.** Shady RAT использует варианты вредоносного ПО, которое используется многие годы.

Shady Rat: вопросы

- **Доказательства причастности конкретных стран.** Заголовки желтой прессы типа "Китай подозревается в атаках Shady RAT ," являются дезинформацией. (Данный пример стал результатом предположения бывшего адвоката правительства США, высказанного журналисту.
- **Что происходит с похищенными данными.** Резонно предположить, что данные, собранные Shady RAT — возможно петабайты информации — используются для получения конкурентных преимуществ, которые могут оказать обширный эффект на мировую экономику, рынок труда и вопросы национальной безопасности
- **Сколько атак осталось не выявленными или неразглашенными.** Поскольку атаки происходили из одного центра управления и контроля, можно предположить, что существуют иные подобные центры. Возможно, мы увидели лишь вершину айсберга повсеместной кражи информации.
- **Когда началась атака.** Log-файлы были изучены только начиная с 2006 год. Предполагается, атаки начались гораздо раньше.

Итоги по Shady Rat

2011 год может быть назван "Годом Хакеров" в связи с обнаружением Операции Shady RAT. В дополнение к этому наблюдается растущая активность хакерских атак — и это лишь в середине года.

Отчет McAfee Inc. (NYSE: MFE) не сфокусирован на произошедшем всплеске атак с целью кражи данных, от которых пострадали RSA и Sony, или самоанонсированных взломах Lulz и Anonymous. Он посвящен операции Shady RAT (Remote Access Tool – средство удаленно доступа), которая была выявлена при анализе протоколов с сервера управления и контроля, начиная с середины 2006 до середины 2010 годов.

В результате изучения log-файлов были обнаружены интенсивные атаки и проникновения в сеть 72 организаций в 14 различных странах. Среди жертв имеются подрядчики оборонных систем США и Великобритании, производитель электронной продукции Сингапура, Олимпийский комитет и корейская сталепрокатная компания.

Дмитрий Альперович, вице-президент по исследованию угроз в McAfee, сделал следующее заключение: "Несмотря на то, что обширность и продолжительность атак Shady RAT может шокировать тех, кто не принимал непосредственного участия в исследовании данных инцидентов, я бы хотел еще раз подчеркнуть, что это была конкретная операция, которой управлял один человек или группа людей».

Позитивным моментом следует считать открытость McAfee, опубликовавшей множество фактов и данных относительно этого происшествия. Слишком долго данная информация была секретом. Осведомленность все-таки является важной частью защиты.

Наконец, следует отметить, что подобная тематика всегда приводит к неадекватным публикациям, заголовки которых отражают догадки мало информированных людей. Например, если Китай не был подвержен атаке – значит, за взломы несет ответственность правительство Китая? Что же, Франция, Индонезия или Гренландия также не пострадали – может быть стоит обвинить и эти страны?

Как сказал Лорд Джефри (1773 - 1850), шотландский адвокат и литературный критик: "Опасайтесь предубеждений. Они как крысы, а умы людей – как ловушки; предубеждения попадают туда легко, но сомнительно, что они выйдут оттуда когда-нибудь".

Развитие GHOSTинга — абузоустойчивый хостинг в облаках

Все больше киберпреступников предлагают клиентам услуги абузоусойчивого хостинга, используя VPN (виртуальные честные сети) / VPS (виртуальные частные серверы), которые позволяют осуществлять все виды вредоносной деятельности в сети – вредоносное ПО, ботнеты, фишинг и спам.

По всем признакам данный хостинг выглядит чистым и безопасным, так как никаких вредоносных признаков не обнаруживается на серверах провайдера; реальная угроза находится далеко от серверов и скрыта от расследований основного провайдера.

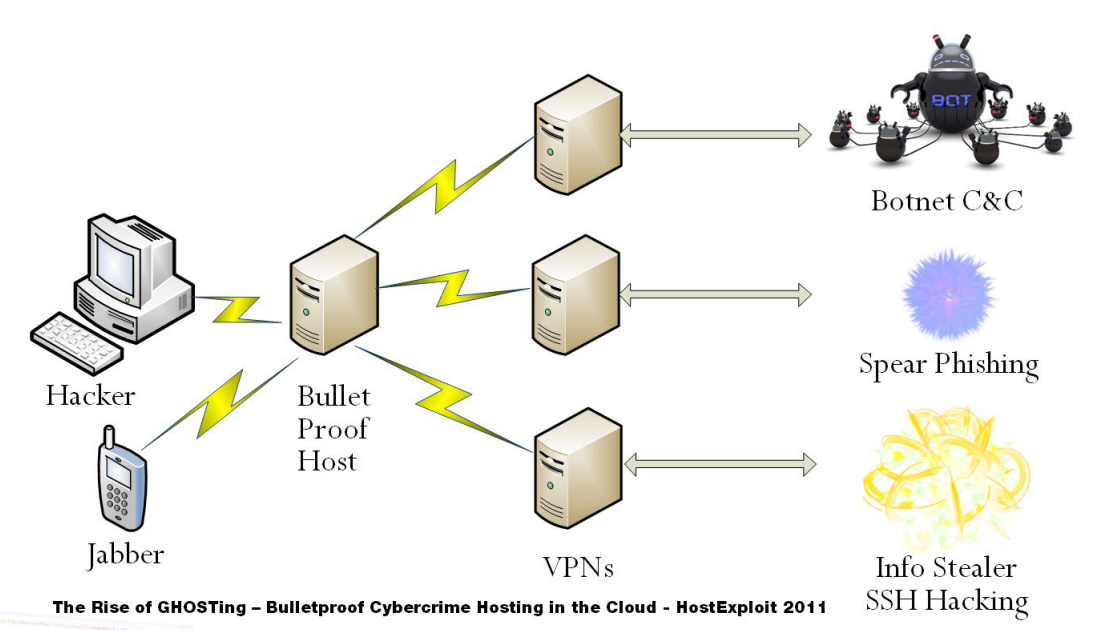


Рис 1 – GHOSTинг – абузоустойчивый хостинг

Работая по такой схеме, реальный хост является лишь получателем нелегального материала или украденных данных и может заявлять о том, что не знает ни о каких происшествиях. Например, коммерческий GHOSTинг имеет строгие правила, регламентирующие, что может быть размещено на реальном абузоустойчивом хостинге, а что – нет:

Допустимый контент:

- Материалы для взрослых
- Ботнеты
- Страницы для загрузчиков, эксплойтов
- ПО манипулирующее с трафиком
- Входящий спам и данные

Запрещенный контент:

- Детская порнография
- Терроризм
- Исходящий спам
- Локальное хранение реальных эксплойтов – только через специальные VPN/ VPS.

Платежи за хостинг производятся через стандартные системы, такие как LibertyReserve, PerfectMoney, WebMoney и т.д. Это снижает риск прекращения деятельности абузоустойчивого хостинга, позволяя клиентам работать, ведь срок жизни виртуальных VPN /VPS может быть меньше, чем требуется правоохранительным органам для выявления провайдера и прекращения его деятельности.

Введение

Введение

Третий квартал 2011 года приходит на смену первой половине года, которая была наполнена сообщениями о взломах и утечках данных.

В сентябре стало известно, что данные кредитных карт клиентов Betfair были украдены через AS16096 Betfair the Sporting Exchange Ltd. (Великобритания), что стало причиной для беспокойства, однако в то же время было выяснено, что инцидент произошел еще 18 месяцев назад. Ни один из клиентов Betfair не был проинформирован об инциденте, а после этого поступило сообщение, что информация не была опубликована из-за нежелательных изменений на бирже ценных бумаг.

Компания DigiNotar (Нидерланды) стала еще одним примером уже слишком привычной истории о слишком медленной реакции на событие, которое оказалось действительно серьезной хакерской атакой и утечкой данных. 531 поддельный сертификат и срочное обновление от Microsoft, блокирующее все сертификаты DigiNotar оказалось слишком тяжелым ударом для компании. Потеряв свои активы и репутацию, организация начала процедуру банкротства в судах Голландии в конце сентября 2011 года.

Jart Armin

Ботнет Kelihos и его чешский хостинг

В третьем квартале поступили приятные новости от Корпорации Microsoft, объявившей, что ботнет Kelihos (Waledac 2.0) был отключен. Впервые Microsoft начала преследование ответчика за подобное правонарушение в рамках гражданского дела – Dominique Alexander Piatti, dotFREE Group S.r.o и 22 John Does были признаны ответственными за запуск и контроль ботнета Kelihos. Домен верхнего уровня cz.cc использовался для регистрации субдоменов и был широко известен размещением различного типа вредоносного контента. За эту деятельность он был отключен 26 сентября 2011 года.

Республика Чехия, в которой размещалась сеть ботнета Kelihos, уже не первый раз дает пристанище плохим хостам, в частности там работали два провайдера, постоянно присутствующие в рейтинге 100 самых плохих хостов. AS24971 Master Internet s.r.o. в настоящее время размещает C&C серверы и спам-боты, распространяя вредоносные URL и прочий нежелательный контент. История активности на SiteVet отражает пики вредоносной активности Master Internet, которые стали больше, чем обычно, в сентябре 2011 года.

AS39392 SuperNetwork s.r.o. — крупнейший провайдер контента в Чехии, смог понизить свои позиции в рейтнге самых плохих хостов, заняв в этом квартале 64 место, но по-прежнему рассылает недопустимое количество спама, вредоносных URL, эксплойтов и другого нежелательного контента.

Говоря о количестве плохих хостов, республика Чехия является маленьким игроком, но поддержка ботнетов несет угрозу широкого распространения в зависимости от количества компьютеров, которые удастся захватить. В случае с Kelihos, 45,000 компьютеров и 4 миллиарда спам-сообщений в день стали достаточным основанием, чтобы прекратить его деятельность.

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.

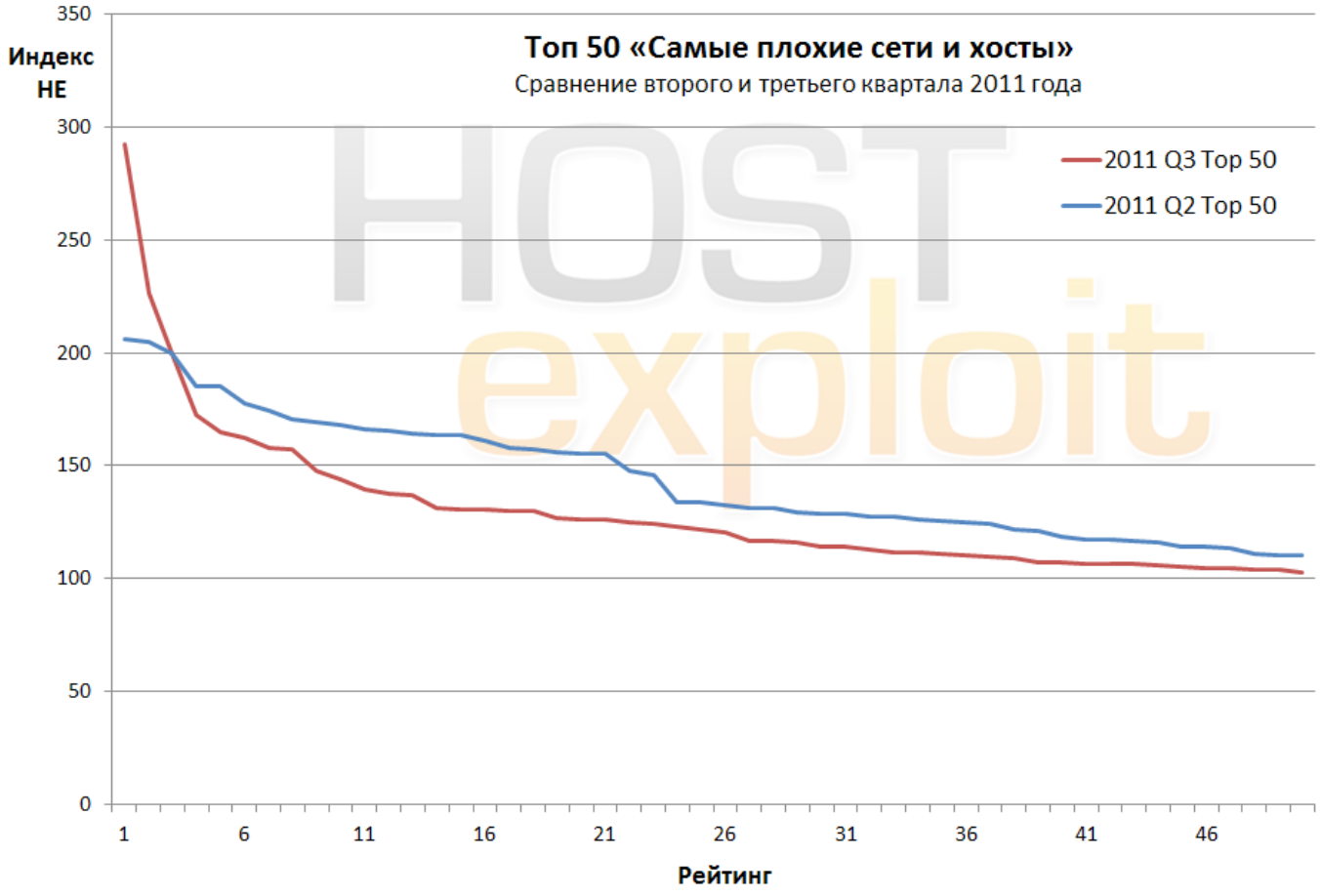
Обратная связь приветствуется!

contact@hostexploit.com | info@group-ib.ru

3. Топ 50

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
1	292.7	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
2	226.2	47583	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	3,328
3	200.1	10297	ENET-2 - eNET Inc.	US	90,880
4	172.8	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	43,776
5	164.9	16138	INTERIAPL INTERIA.PL SA	PL	4,096
6	162.6	45899	VNPT-AS-VN VNPT Corp	VN	2,171,136
7	157.9	32475	SINGLEHOP-INC - SingleHop	US	235,264
8	157.0	22489	CASTLE-ACCESS - Castle Access Inc	US	49,408
9	147.8	16276	OVH OVH Systems	FR	548,864
10	143.9	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
11	139.7	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,548,288
12	137.8	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	943,104
13	137.3	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	108,295,136
14	131.1	13727	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024
15	130.4	24940	HETZNER-AS Hetzner Online AG RZ	DE	502,784
16	130.4	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,640
17	130.3	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	IN	254,976
18	129.8	9809	NOVANET Nova Network Co.LtdRoom 1205... Shenzhen, China	CN	10,240
19	126.7	41947	WEBALTA-AS OAO Webalta	RU	15,872
20	126.3	29550	SIMPLYTRANSIT Simply Transit Ltd	GB	106,496
21	125.9	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San.	TR	14,592
22	124.9	43146	AGAVA3 Agava Ltd.	RU	17,408
23	124.2	3595	GNAXNET-AS - Global Net Access, LLC	US	155,136
24	123.3	16265	LEASEWEB LeaseWeb B.V.	NL	279,808
25	121.6	11798	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	145,408
26	120.3	40824	WZCOM-US - WZ Communications Inc.	US	9,216
27	116.8	6697	BELPAK-AS BELPAK	BY	1,075,200
28	116.5	6849	UKRTELNET JSC UKRTELECOM,	UA	1,507,840
29	116.0	19318	NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE	US	90,368
30	114.1	15169	GOOGLE - Google Inc.	US	282,112
31	114.0	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	129,792
32	112.7	29873	BIZLAND-SD - The Endurance International Group, Inc.	US	96,768
33	111.6	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
34	111.3	17971	TMVADS-AP TM-VADS Datacenter Management	MY	40,576
35	110.9	25532	MASTERHOST-AS .masterhost autonomous system	RU	78,336
36	110.2	21788	NOC - Network Operations Center Inc.	US	278,528
37	109.9	9829	BSNL-NIB National Internet Backbone	IN	7,664,640
38	108.8	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512
39	107.2	9318	HANARO-AS Hanaro Telecom Inc.	KR	14,982,912
40	107.0	15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,672
41	106.8	29497	KUBANGSM CJSC Kuban-GSM	RU	21,760
42	106.5	16125	DC-AS UAB Duomenu Centras	LT	5,376
43	106.2	12322	PROXAD Free SAS	FR	12,271,616
44	105.8	9050	RTD ROMTELECOM S.A	RO	1,648,896
45	105.0	8661	PTK PTK IP	RS	57,344
46	104.7	8972	PLUSSERVER-AS PlusServer AG, Germany	EU	147,456
47	104.5	13301	UNITEDCOLO-AS UNITED COLO GmbH	DE	66,816
48	103.8	6903	ZENON-AS ZENON N.S.P.	RU	32,768
49	103.7	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,916,160
50	102.8	13213	UK2NET-AS UK-2 Ltd Autonomous System	EU	54,528

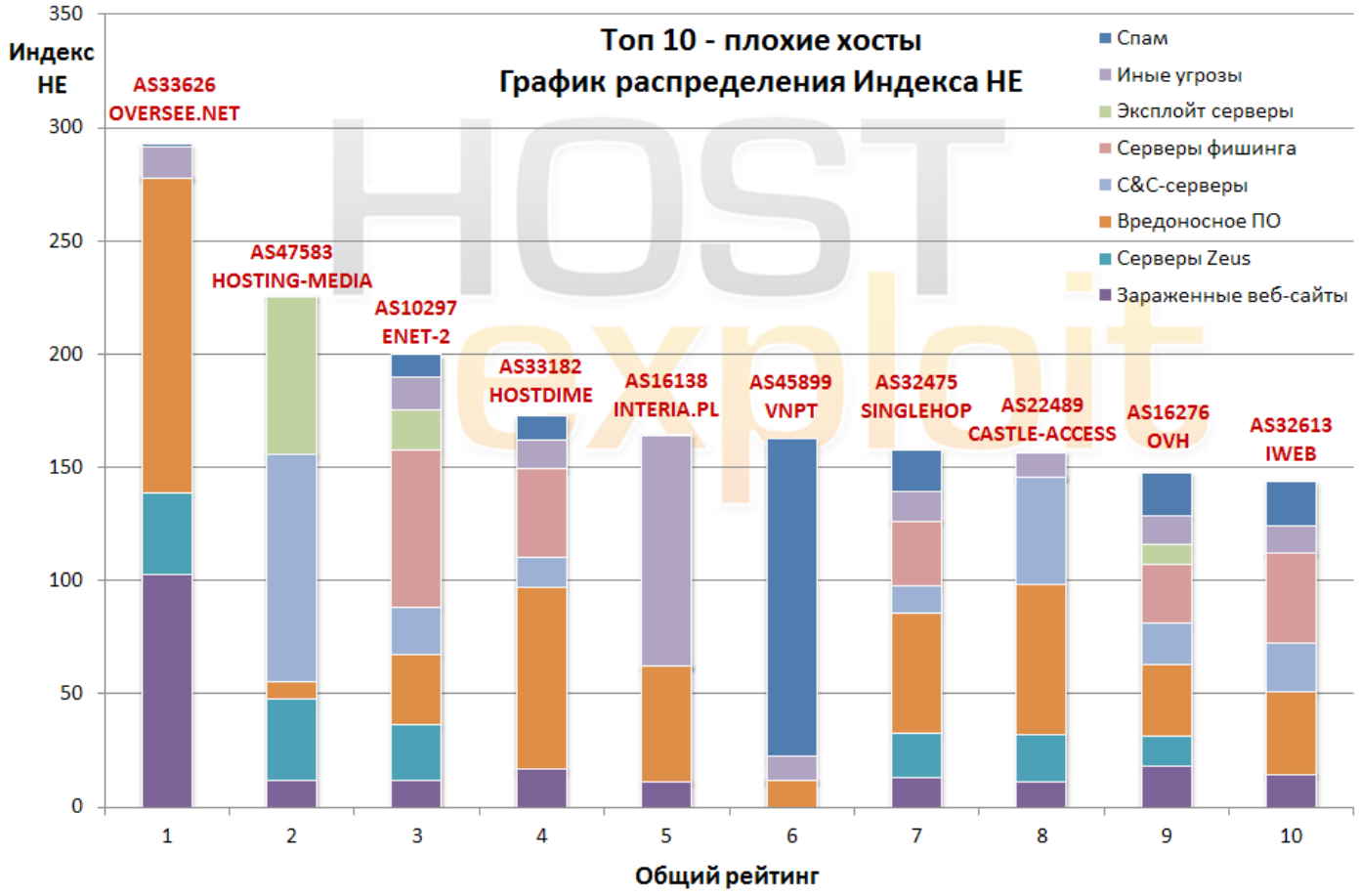
Сравнение первого и второго квартала 2011 года



Сравнения рейтинга Топ 50 «Самых плохих хостов» в июне 2011 года и в сентябре 2011 года.

Реальный уровень нежелательных объектов стал более сконцентрированным на самых плохих серверах в этом квартале, в то время как общий уровень рейтинга Топ 50 остался примерно прежним.

Топ 10. График распределения Индекса НЕ



Снижение Индекса НЕ, которое вы можете видеть для Топ 10 «Самых плохих хостов», говорит о следующем:

Во-первых, учет веса различных категорий говорит о том, что Индекс НЕ является сбалансированным показателем, а значит ни один из видов угроз не доминирует над другими.

Во-вторых, данная тенденция демонстрирует распределение Индекса НЕ для каждой отдельной категории АС в списке Топ 10, что объясняет, почему каждый из них имеет столь высокий рейтинг.

Например, вы можете видеть, что AS33626 Oversee.net (US) имеет рейтинг #1, так как в основном данный узел размещает вредоносное ПО и зараженные веб-сайты, демонстрируя меньшую концентрацию Zeus и других событий.

AS45899 VNPT (US), с другой стороны, попал в Топ 10 за счет распространение большого количества спама.

Новое за квартал

6.1. Обзор

	Предыдущий квартал - Q2 2011			Текущий квартал - Q3 2011		
	Номер	Название АС	Страна	Номер	Название АС	Страна
#1	33182	HostDime	US	33626	Oversee.net	US
#2	29073	Ecatel	NL	47583	Hosting Media	LT
#3	10297	eNET	US	10297	eNET	US
#1 Спам	33774	DJAWEB	DZ	45899	VNPT Corp	VN
#1 C&C-серверы	36408	Panther Express / CDNetworks	US	47583	Hosting Media	LT
#1 Серверы Zeus	41947	Webalta	RU	16125	Duomenu Centras	LT
#1 Серверы фишинга	10297	eNET	US	10297	eNET	US
#1 Эксплойт серверы	14585	CIFNet Inc.	US	47583	Hosting Media	LT
#1 Вредоносное ПО	33626	Oversee.net	US	33626	Oversee.net	US
#1 Зараженные веб-сайты	29073	Ecatel	NL	33626	Oversee.net	US
#1 Иные угрозы	16138	Interia.pl	PL	16138	Interia.pl	PL

В этом квартале произошли значительные изменения на некоторых хостах, ранее регулярно входивших в Топ 10. Особенно приятно видеть, что AS29073 Ecatel окончательно вышел из этого списка и занял позицию #53.

Ecatel присутствовал в Топ 10 с начала 2010 года. Мы всегда верили в возможность позитивных изменений и поэтому выражаем наши поздравления Ecatel и надеемся, что компания продолжит снижать свои позиции в рейтинге.

Новичок на позиции #1 — американский провайдер AS33626 Oversee.net, который также стал #1 в категории вредоносное ПО и по количеству зараженных сайтов, в то время как AS47583 Hosting Media, занимающий место #2 в общем рейтинге, является #1 по категориям ботнет и эксплойт-серверы.

6.2. Топ 10. Вновь зарегистрированные хосты

К концу третьего квартала 2011 года было обнаружено **39,056** автономных систем; что на **1,056** больше чем было в конце второго квартала 2011 года.

Ниже приведена выборка 10 автономных систем с самым высоким Индексом НЕ, зарегистрированных в третьем квартале 2011 года. Учитывая большое количество плохого контента, обнаруженного за короткий промежуток времени, данные хосты представляют собой большой интерес.

Под списком 10 автономных систем из третьего квартала вы можете видеть такие же списки, отражающие исследования предыдущих двух кварталов. Как вы можете видеть, автономные системы в данном квартале отличаются от предыдущего квартала — они имеют больший диапазон адресов. Ожидается, что новые хосты, на которых замечены значительные уровни вредоносной активности, являются «одноразовыми» АС, изначально рассчитанными на малый срок жизни. Также происходило до третьего квартала с двумя крупными автономными системами на Тайване и одним в Китае.

	Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP
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
2011 Q1	92	98.3	47306	ISEC-AS The International Scientifical and Educational Centre	UA	256
	309	67.4	42741	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	RO	1,280
	359	64.0	43134	COMPLIFE-AS CompLife Ltd	MD	512
	657	52.9	20228	PACNET-MX - Pacnet, S.A. de C.V.	US	12,288
	677	52.2	16109	INCA-AS Informational and Commercial Agency "INCA" LTD	UA	256
	827	47.5	8514	INODE UPC Austria GmbH	AT	0
	1,481	34.1	51786	SATURN-R-GROUP LLC Telecom-Group-Saturn_R	RU	1,536
	1,779	29.5	55831	AIRCEL-IN Aircel Ltd.	IN	177,152
	1,854	28.6	51362	BESTISP-AS PE Yastremskiy Leonid Stepanovich	UA	512
	1,927	27.7	52116	ORIONTELEKOMTIM-AS Orion Telekom Tim d.o.o.Beograd...	RS	8,192

6.3. Вылеченные хосты

Изменение	Предыдущий квартал		Текущий квартал		Номер	Название АС	Страна	Количество IP
	Рейтинг	Индекс	Рейтинг	Индекс				
-99.1%	24	133.8	30,277	1.2	50693	KONSING-GROUP Konsing group doo	RS	2,048
-98.5%	112	84.6	11,137	1.3	49130	ARNET-AS SC ArNet Connection SRL	EU	0
-95.2%	62	105.5	6,021	5.0	50244	ITELECOM Pixel View SRL	RO	8,704
-83.2%	109	85.2	3,440	14.3	50465	IQHOST IQHost Ltd	RU	3,584
-80.4%	49	110.3	2,284	21.7	51306	UAIP-AS PAN-SAM Ltd.	UA	2,048
-77.5%	84	95.1	2,337	21.4	37957	CNNIC-CCCNET China Communication	CN	4,096
-69.8%	33	127.2	1,050	38.5	39150	TRANSIT-TELECOM-AS Tranzit Telecom	UA	5,376
-68.1%	17	157.8	555	50.3	33774	DJAWEB	DZ	1,707,776
-65.7%	16	161.1	437	55.2	6851	BKCNET "SIA" IZZI	LV	49,152
-64.8%	48	111.0	1,019	39.0	14585	CIFNET - CIFNet, Inc.	US	7,680

Хосты, указанные в таблице выше, все без исключения продемонстрировали значительное снижение содержания нежелательного контента за три месяца, прошедшие с момента выпуска предыдущей версии отчета - с конца второго квартала 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. Но все перечисленные компании еще раз подтверждают реальную возможность снижения количества нежелательных компонентов, если вы готовы приложить дополнительные усилия и думать не по шаблону.

Среди хостов, улучшивших свои позиции:

- AS50693 Konsing Group (RS) спустился вниз с позиции #24 до #30,277, показав сокращение количества вредоносного контента на 99,1%.
- AS49130 Arnet Connection (EU) снизил свои позиции в рейтинге на 98,5%, достигнув незначительного количества вредоносного контента.
- AS50244 ITelecom (RO) улучшил положение на 95,2%, полностью покинув рейтинг Топ 100.

6.4. Хосты, состояние которых ухудшилось

Изменение	Предыдущий квартал		Текущий квартал		Номер	Название AC	Страна	Количество IP
	Рейтинг	Индекс	Рейтинг	Индекс				
22,610.1%	31,461	1.0	2	226.2	47583	HOSTING-MEDIA Aurimas Rapalis	LT	3,328
668.9%	3,293	14.5	33	111.6	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
362.6%	2,628	19.0	90	88.0	10922	LIVEJOURNAL - Live Journal Inc.	US	1,024
172.5%	1,330	34.0	78	92.6	55330	GCN-DCN-AS AFGHANTELECOM...	AF	14,592
162.9%	1,536	30.4	115	80.0	20648	RAN-NETWORKS RAN Networks S.L.	ES	8,192
136.9%	831	44.1	47	104.5	13301	UNITEDCOLO-AS UNITED COLO GmbH	DE	66,816
136.4%	1,019	40.4	70	95.5	9280	CIA-AS connect infobahn australia...	AU	8,704
112.8%	691	47.5	51	101.0	39570	LOOPIA Loopia AB	SE	768
109.2%	225	68.8	10	143.9	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
101.2%	499	54.1	38	108.8	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512

Хосты, перечисленные в данном разделе, показали наиболее интенсивный рост вредоносного содержимого по сравнению с предыдущим кварталом. Новые хосты были отмечены в отдельной секции (6.2).

Самый “выдающийся” хост данного квартала - AS47583 Hosting Media, показавший максимальный рост вредоносного содержимого. Ранее занимавший место в нижней части рейтинга, провайдер Hosting Media перепрыгнул на #2 место по общему уровню активности киберпреступников, а также занял #1 место в категориях ботнеты и эксплойт-серверы.

Второе место по ухудшению состояния занял хост AS8660 Matrix S.p.a., переместившийся на позицию #33. При этом Matrix S.p.a. лидирует по количеству фишинга (#2 место), а также размещает злонамеренных URL, вредоносное ПО, ботнетов и поддерживает прочие угрозы.

AS10922 Live Journal Inc. достиг позиции #90 за размещение злонамеренных URL, вредоносного ПО и прочих угроз.

Всем хостам, перечисленным в данном разделе, было рекомендовано пересмотреть недавно примененные изменения, которые могли привести к такому росту вредоносной активности.

Анализ по странам

В данном квартальном отчете мы расширили таблицу распределения плохих хостов по странам, включив в нее 250 автономных систем вместо 50.

В списке стран имеются как регионы с высокой злонамеренной активностью, так и те, в которых просто имеется большое количество хостов.

Чтобы учесть этот нюанс мы разработали уникальную технологию, позволяющую более точно определить уровень злонамеренной активности в стране. При этом пришлось разбираться с новым спектром сложностей, в частности — невозможностью корректного определения физического местоположения сервера в автоматическом режиме.

"Индекс страны" отражает уровень злонамеренной активности по шкале из 1000 баллов и незначительно зависит от количества хостов, находящихся в конкретной стране.

Фактически, данный показатель отражает уровень злонамеренной активности, также как Индекс НЕ отражает уровень вредоносности конкретного хоста, не привязываясь напрямую к количеству IP адресов, определенных для данного хоста.

Новый подход позволяет производить более точный анализ перемещения злонамеренной активности между различными странами.

Хосты из Топ 250	Страна	Общее количество IP в Топ 50	Общий индекс	Средний индекс	Средний индекс по категории							
					Зараженные веб-сайты	Серверы Zeus	Вредоносное ПО	C&C-серверы	Серверы фишинга	Эксплойт серверы	Иные угрозы	Спам
60	UNITED STATES	143,109,632	5,712.9	95.2	128.7	59.5	155.4	116.4	85.7	29.8	114.7	40.8
26	RUSSIAN FEDERATION	5,115,328	2,228.1	85.7	82.7	153.9	87.3	52.5	6.1	30.3	82.6	114.7
13	GERMANY	35,424,256	1,156.4	89.0	103.3	105.0	122.1	96.2	70.9	55.3	100.6	48.4
13	CHINA	215,357,856	1,156.3	88.9	89.5	29.5	147.4	112.5	10.5	78.6	103.0	70.8
11	BRAZIL	27,118,080	806.3	73.3	95.3	0.1	101.3	125.7	0.1	29.1	102.5	69.3
10	UNITED KINGDOM	17,348,352	743.5	74.4	105.5	28.1	123.8	86.8	0.1	27.1	109.5	49.1
9	INDIA	11,120,128	788.0	87.6	37.0	0.1	40.7	11.5	0.1	22.0	44.6	313.9
9	UKRAINE	2,242,816	705.2	78.4	80.0	142.6	98.6	74.6	0.2	0.1	105.1	65.8
9	TURKEY	11,368,704	694.5	77.2	96.4	43.1	121.6	51.3	0.1	46.1	102.9	76.2
7	NETHERLANDS	402,688	620.5	88.6	115.6	94.9	125.4	71.2	31.0	101.7	119.8	43.3
6	EUROPE	29,584,896	498.4	83.1	103.6	31.4	117.5	111.5	51.9	0.0	101.0	79.1
5	KOREA, REPUBLIC OF	92,772,032	414.6	82.9	133.9	0.0	93.5	120.7	25.1	99.6	103.7	72.8
4	FRANCE	12,840,960	432.5	108.1	95.7	131.7	188.3	67.5	130.4	58.9	107.9	51.8
4	VIET NAM	6,062,080	393.7	98.4	77.8	0.0	99.8	55.4	0.1	0.0	102.4	241.7
4	CZECH REPUBLIC	391,424	329.6	82.4	111.4	75.3	149.4	83.6	0.1	41.9	105.1	33.4
4	SPAIN	14,407,680	298.9	74.7	105.4	105.2	133.3	25.4	0.1	0.0	101.2	46.7
3	CANADA	373,504	342.7	114.2	78.9	120.5	216.5	103.5	185.1	0.0	105.0	51.0
3	AUSTRALIA	54,784	292.5	97.5	68.1	162.7	97.9	37.2	496.8	0.1	103.4	5.8
3	THAILAND	261,888	233.1	77.7	105.8	117.1	112.3	35.7	0.1	73.8	68.3	62.2

«Чистые» хосты

Рейтинг HE	Индекс HE	Номер	Название AC	Страна	Количество IP
37,382	0.37	38333	SYMBIO-AS-AU-AP Symbio Networks	AU	147,296
37,378	0.38	5605	NETUSE NetUSE AG	DE	140,544
37,363	0.39	19855	ASN-MASERGY-US Masergy US Autonomous System	US	131,840
37,356	0.39	2895	FREE-NET-AS FREEnet	EU	131,072
37,324	0.42	23329	AS-OPENACCESS - Open Access Inc.	US	112,384
37,276	0.46	16811	SPACENET-GTH - Spacenet, Inc.	US	913,152
37,246	0.48	2594	ASN-CSI CSI Piemonte	EU	81,920
37,079	0.53	2685	ASATTCA AT&T Global Network Services - CA	US	65,536
37,065	0.54	35776	TELEOS Teleos	DE	62,464
36,815	0.64	71	HP-INTERNET-AS Hewlett-Packard Company	US	35,072,000

8.1. 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.

8.2. 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

9.1.1. Серверы управления ботнетами

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
2	226.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	3,328	**937.6**
26	120.3	**40824**	WZCOM-US - WZ Communications Inc.	US	9,216	**621.9**
87	88.6	**36408**	ASN-PANTHER Panther Express	US	80,384	**579.0**
8	157.0	**22489**	CASTLE-ACCESS - Castle Access Inc	US	49,408	**441.6**
848	42.4	**29990**	ASN-APPNEXUS - AppNexus, Inc	US	34,816	**391.7**
747	44.8	**37963**	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co., Ltd.	CN	762,880	**263.3**
1,376	31.9	**42173**	YAHOO-SWITZERLAND Yahoo! Europe	GB	15,104	**262.8**
65	96.2	**27715**	LocaWeb Ltda	BR	83,200	**224.9**
515	51.7	**47764**	MAILRU-AS Limited liability company Mail.Ru	RU	12,032	**206.5**
10	143.9	**32613**	IWEB-AS - iWeb Technologies Inc.	CA	218,112	**206.1**

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 улучшилась по сравнению со 2 кварталом: в этот раз США представлена 4 местами в списке Топ 10 худших хостов по размещению управления ботнетами, тогда как в прошлом квартале их было 6.

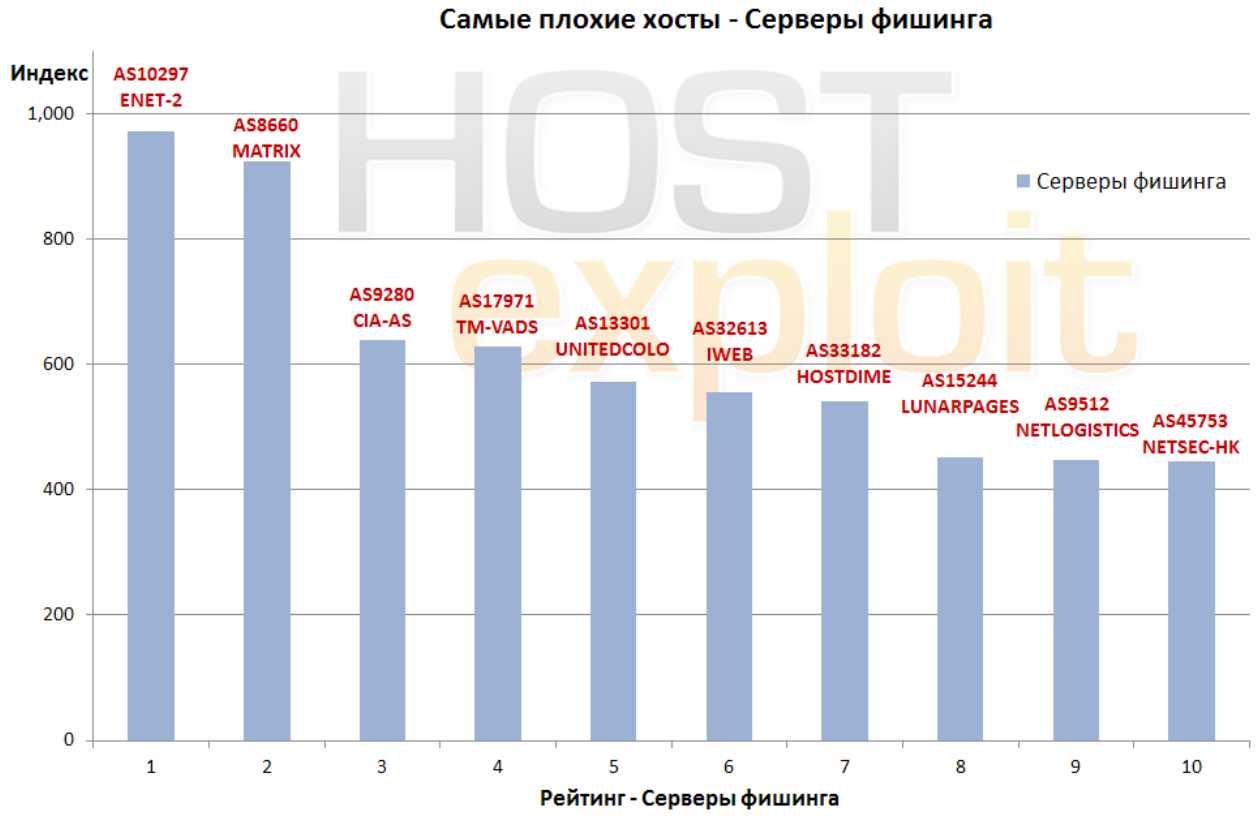
9.1.2. Серверы фишинга

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
3	200.1	**10297**	ENET-2 - eNET Inc.	**US**	90,880	**971.6**
33	111.6	**8660**	MATRIX-AS Matrix S.p.A.	**IT**	8,192	**924.0**
70	95.5	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,704	**639.9**
34	111.3	**17971**	TMVADS-AP TM-VADS Datacenter Management	**MY**	40,576	**628.4**
47	104.5	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816	**572.9**
10	143.9	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	218,112	**555.0**
4	172.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**540.6**
16	130.4	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	48,640	**452.6**
89	88.2	**9512**	NETLOGISTICS-AU-AP Net Logistics Pty. Ltd.	**AU**	13,568	**448.1**
74	94.4	**45753**	NETSEC-HK Unit 1205-1207	**HK**	117,504	**444.7**

Фишинг и социальный инжиниринг остаются основными источниками проблем для банков и корпораций всех размеров.

В прошедшем квартале основные 6 хостов, занимающихся фишингом, были обнаружены в США. Теперь их количество сократилось до 3.

Вредоносный код, размещенный на серверах западных стран, сводит к минимуму подозрительность заказчиков и организаций, позволяя создать ложное впечатление надежности, что и является краеугольным камнем кампаний фишинга.



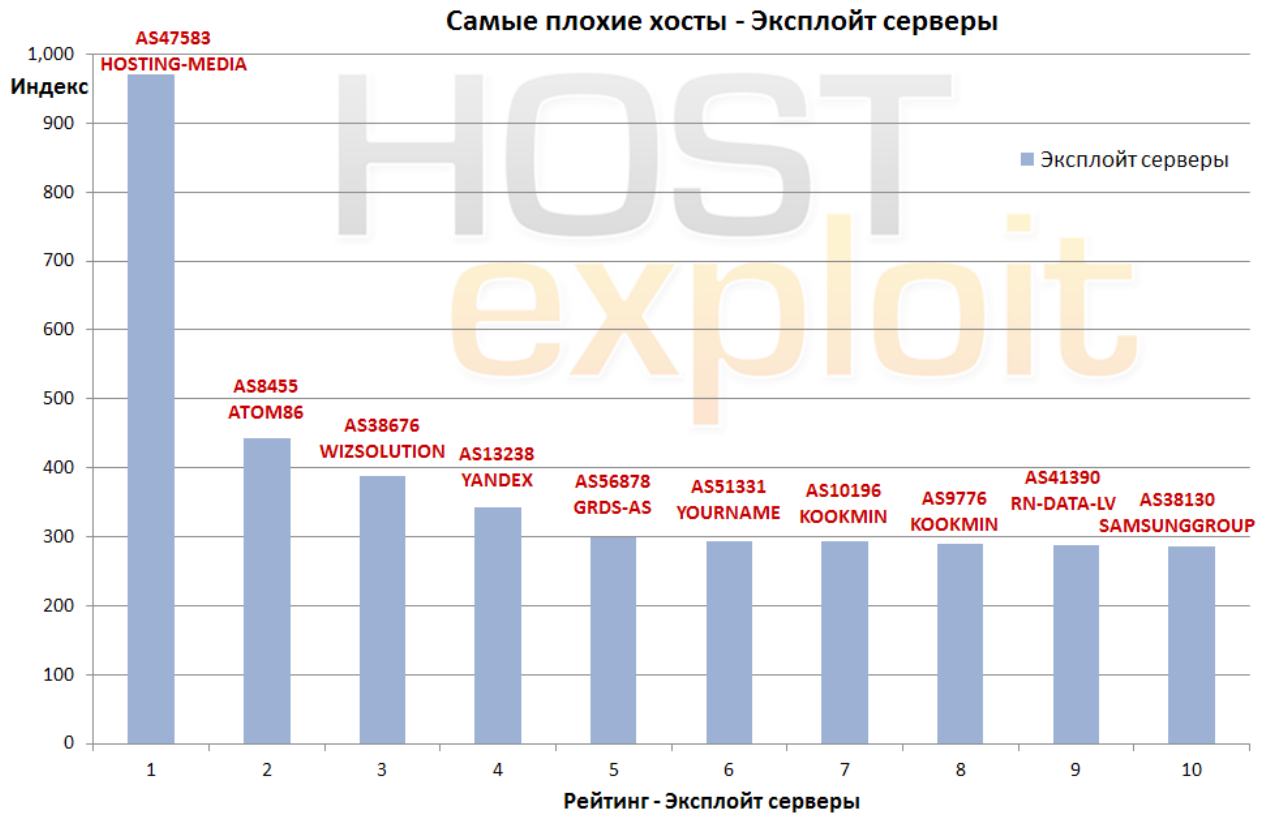
9.1.3. Эксплоит-серверы

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
2	226.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	3,328	**971.5**
146	73.8	**8455**	ATOM86-AS ATOM86 Autonomous System	**NL**	17,408	**442.2**
517	51.6	**38676**	AS33005-AS-KR wizsolution co.,Ltd	**KR**	8,704	**388.7**
121	79.0	**13238**	YANDEX Yandex LLC	**RU**	164,480	**341.6**
1,147	36.5	**56878**	GRDS-AS LLC "Inter-Treyd"	**RU**	256	**298.7**
1,271	33.8	**51331**	YOURNAME Your Name Webhosting	**NL**	768	**294.1**
2,214	22.2	**10196**	HNCBWORLD-AS-KR Kookmin Bank	**KR**	768	**294.1**
2,260	21.9	**9776**	KBSTAR Kookmin Bank	**KR**	1,280	**289.8**
270	64.5	**41390**	RN-DATA-LV RN Data, SIA	**LV**	1,536	**287.7**
1,342	32.4	**38130**	SAMSUNGGROUP Samsung Networks Inc.	**KR**	1,664	**286.7**

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

Множество хостов и корпоративных серверов распространяют вредоносное ПО или выполняют другие злонамеренные действия в результате взлома и компрометации. Важная информация, персональные данные жертв и другие данные, полученные нелегальным путем, направляются на данные эксплойт-серверы при помощи вредоносного ПО.

В отличие от хостов, рассылающих спам, ранее эксплойт-серверы в основном находились в странах с недостаточным уровнем государственного регулирования. В этом квартале мы видим возвращение данного тренда по сравнению с предыдущим, когда американские хосты вошли в Топ 10 в категории «Эксплойт-серверы».



9.1.4. Серверы Zeus

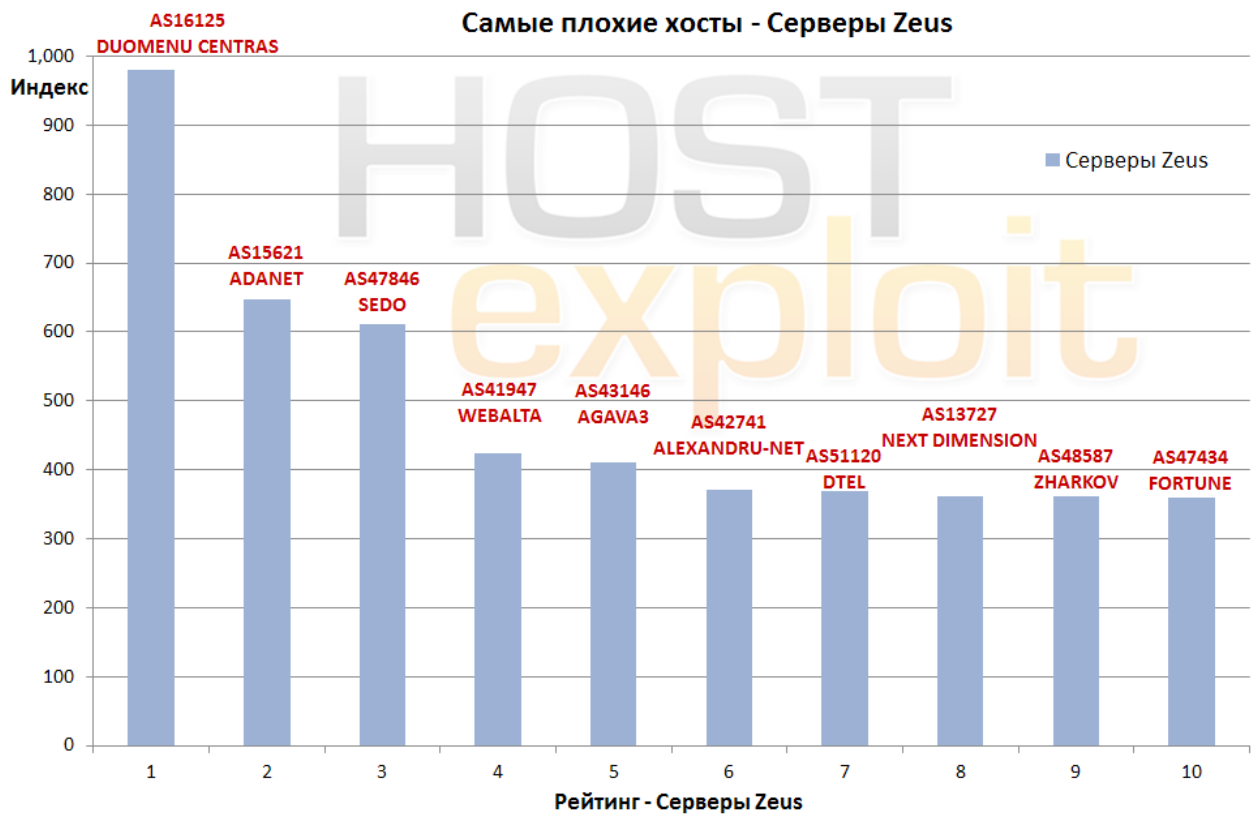
Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
42	106.5	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**980.1**
60	97.3	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	11,264	**647.1**
71	95.4	**47846**	SEDO-AS Sedo GmbH	**DE**	1,536	**611.5**
19	126.7	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,872	**423.1**
22	124.9	**43146**	AGAVA3 Agava Ltd.	**RU**	17,408	**411.4**
918	41.0	**42741**	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	**RO**	256	**370.7**
923	40.8	**51120**	DTEL-BIZ-AS DTEL Inc.	**RU**	384	**369.2**
14	131.1	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**361.6**
185	70.0	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	**UA**	1,024	**361.6**
113	80.5	**47434**	FORTUNE-AS Fortune Science and Production Company	**UA**	1,280	**358.7**

Киберпреступники управляют сетями зараженных компьютеров, также называемых «зомби», через серверы управления ботнетами. С одного такого сервера может управлять примерно 250,000 или более подчиненными машинами. Мы выделили в данном отчете Zeus-ботнет, так как он самый дешевый и популярный на черном рынке.

Этот раздел следует рассматривать совместно с разделом 9.1.3, посвященным эксплойт-серверам.

В списке вы можете найти множество называний, хорошо известных обозревателям и исследователям, в частности, некоторые из них уже были уличены в неправомерных действиях.

Серверы управления и зараженные конечные станции Zeus (Zbot) приводятся в сочетании с данными от известного ресурса, посвященного ботнету Zeus, — abuse.ch.



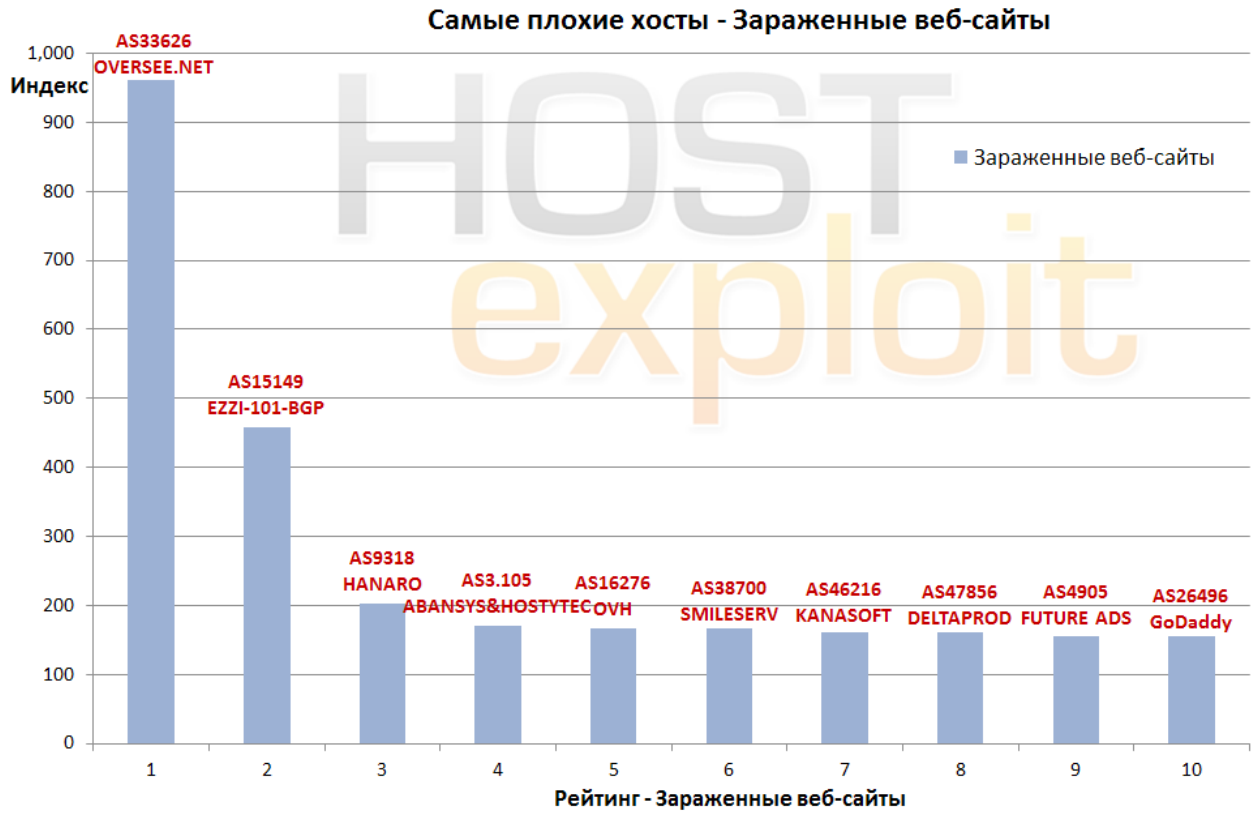
9.2.1. Зараженные веб-сайты

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
1	292.7	**33626**	OVERSEE-DOT-NET - Oversee.net	US	3,840	**960.7**
40	107.0	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,672	**457.1**
39	107.2	**9318**	HANARO-AS Hanaro Telecom Inc.	KR	14,982,912	**202.1**
1,739	26.9	**3.105**	ABANSYS_AND_HOSTYTEC-AS Abansys & Hostytec, S.L.	ES	4,096	**170.5**
9	147.8	**16276**	OVH OVH Systems	FR	548,864	**167.0**
366	60.5	**38700**	SMILESERV-AS-KR SMILESERV	KR	108,800	**165.7**
1,767	26.7	**46216**	KANASOFT - KANA Software, Inc	US	256	**161.6**
2,763	18.5	**47856**	DELTAPROD-AS Delta Productions Ltd	IM	512	**160.9**
2,840	18.0	**4905**	FA-LAX-1 - Future Ads LLC	US	256	**156.1**
58	98.0	**26496**	PAH-INC - GoDaddy.com, Inc.	US	1,287,424	**155.7**

Зараженные веб-сайты — это обширная категория ресурсов, где могут сочетаться несколько видов угроз – от вредоносного контента до кражи данных пользователей.

В этом разделе данные нашего собственного исследования, собранные из различных ловушек, представлены в сочетании с данными MalwareURL и hphosts по вредоносным URL-адресам в отдельных автономных системах. Данные от MalwareURL сами по себе агрегируют информацию из нескольких наблюдательных ресурсов.

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

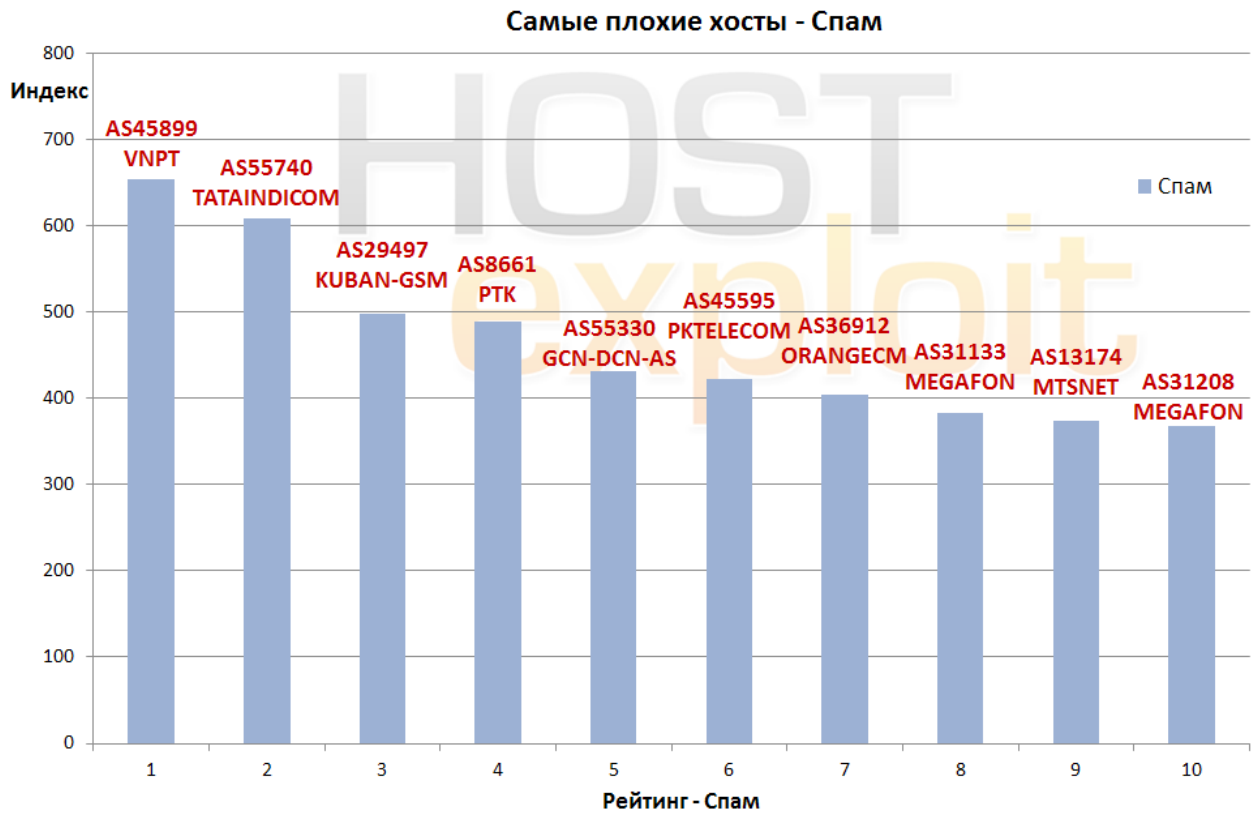


9.2.2. Спам

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
6	162.6	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,171,136	**653.7**
17	130.3	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA	**IN**	254,976	**607.9**
41	106.8	**29497**	KUBANGSM CJSC Kuban-GSM	**RU**	21,760	**498.0**
45	105.0	**8661**	PTK PTK IP	**RS**	57,344	**489.5**
78	92.6	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMM...	**AF**	14,592	**431.5**
73	95.1	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,745,536	**422.3**
94	86.7	**36912**	ORANGECM	**CM**	8,192	**403.7**
77	92.9	**31133**	MF-MGSM-AS OJSC MegaFon	**RU**	16,960	**382.5**
103	83.3	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous System	**RU**	24,320	**374.5**
122	78.9	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	3,072	**367.5**

Список Top 10 по категории спама отражает расположение серверов, наиболее активно используемых для рассылки нежелательных писем. Страны, минимально регулирующие и отслеживающие подобные действия, позволяют спамерам использования многократно опробованные методы для обхода детектирования писем, 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 больше урона, чем целая группа серверов. Более того, небольшое количество спама может быть более эффективно, чем массовая рассылка, если исполнитель применяет специальные технологии подбора адресатов. Эти две особенности делают затруднительной количественную оценку в категории «спам». Поэтому мы совместили данные об известных 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.



9.2.3. Иные угрозы

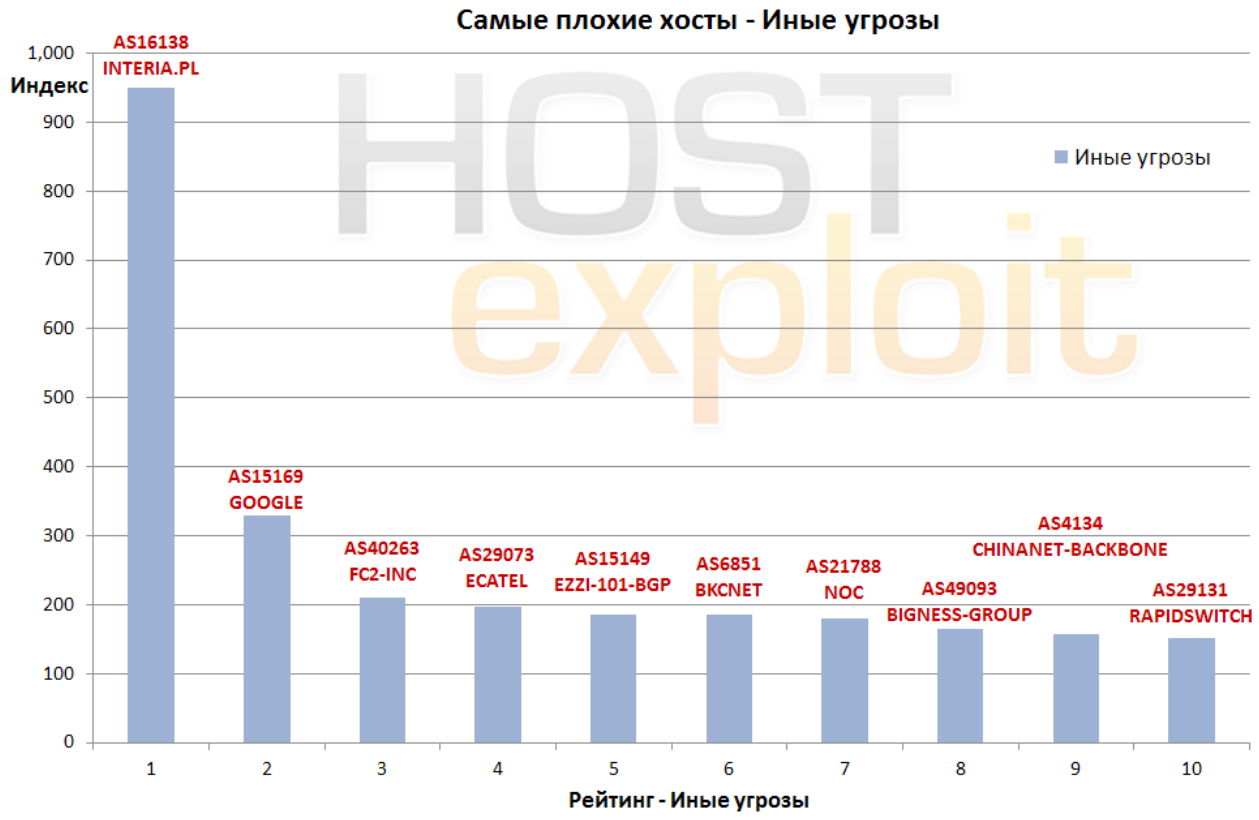
Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
5	164.9	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**949.5**
30	114.1	**15169**	GOOGLE - Google Inc.	**US**	282,112	**329.0**
197	68.9	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.7**
52	100.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.1**
40	107.0	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**186.1**
437	55.2	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.3**
36	110.2	**21788**	NOC - Network Operations Center Inc.	**US**	278,528	**179.0**
2,696	18.8	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	256	**164.3**
13	137.3	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	108,295,136	**157.7**
215	67.6	**29131**	RAPIDSWITCH-AS RapidSwitch	**GB**	0	**152.3**

Это наиболее современная категория быстро меняющихся эксплойтов и векторов атак, отнесенных к прочим угрозам.

Здесь приведены различные вредоносные компоненты эксплойтов, например MALfi (XSS/RCE/RFI/LFI), XSS-атаки, накрутка кликов, черный фарм-бизнес, поддельные антивирусы, Zeus (Zbota), Artro, SpyEye, Stuxnet, черный SEO, Koobface и новые вредоносные инструменты.

Широкий спектр техник из данной категории отражен в рейтинге Топ 10 «Прочих Угроз», в нем вы сможете найти несколько хорошо известных имен

Также как и во втором квартале 40% из Топ 10 находятся в США.



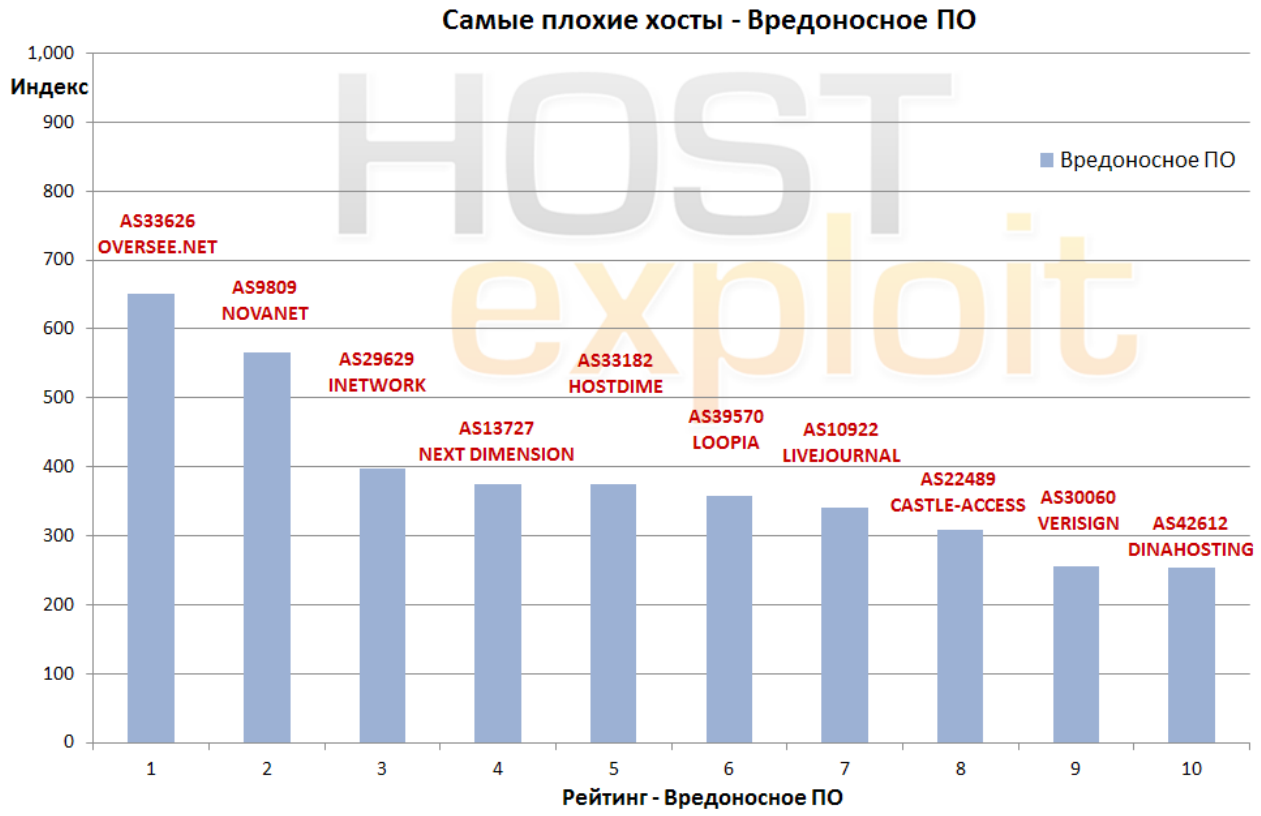
9.2.4. Вредоносное ПО

Рейтинг НЕ	Индекс НЕ	Номер	Название АС	Страна	Количество IP	Индекс из 1000
1	292.7	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**650.1**
18	129.8	**9809**	NOVANET Nova Network Co.Ltd... Shenzhen, China	**CN**	10,240	**566.6**
59	97.6	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**397.2**
14	131.1	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**375.3**
4	172.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**374.3**
51	101.0	**39570**	LOOPIA Loopia AB	**SE**	768	**357.5**
90	88.0	**10922**	LIVEJOURNAL - Live Journal Inc.	**US**	1,024	**340.9**
8	157.0	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**309.3**
236	66.4	**30060**	WILDCARD-VERISIGN - VeriSign Infrastructure & Operations	**US**	5,376	**254.9**
119	79.1	**42612**	DINAHOSTING-AS ASN de Dinahosting SL	**ES**	18,432	**253.9**

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, отраженных в данном отчете.

Результаты исследования в данной категории были основаны главным образом на данных StopBadware, которые, в свою очередь, агрегируют информацию от Google, Sunbelt Software, и Team Cymru.



Выводы

Социальный инжиниринг был признан наиболее опасным трендом для организаций и представителей бизнеса любого масштаба. Большинство из них не имеют необходимых ресурсов для борьбы с новой многоликой угрозой. Увеличение количества персональных устройств, используемых на рабочем месте, приводит к появлению целого спектра проблем. Ключевым аспектом в борьбе с киберпреступностью, проявляющей себя в различных формах, является информирование и предупреждение пользователей/сотрудников/ИТ-специалистов о новых угрозах и потенциальных источниках их появления.

Наш подход к данному вопросу всегда заключался в том, чтобы выделить хосты, которые ненамеренно или специально поддерживают распространение угроз, заполонивших интернет. Мы стремимся привить хостерам ответственность, которую уже приняли на себя многие компании. Однако всего несколько хостов могут испортить репутацию многим, в попытке заработать больше денег, не заботясь ни о чем более.

В заключение об отчете за третий квартал 2011 года мы хотели бы отметить несколько изменений, достойных внимания.

Например, изменения в списке Топ 10 плохих хостов продемонстрировали, что США больше не доминируют в рейтинге, хотя большинство 5 из 10 худших провайдеров все же относятся к Штатам. В рейтинге Топ 50 доля США снизилась до 16% по сравнению с предыдущим показателем в 23% в третьем квартале, и мы надеемся, данный тренд продолжится и дальше. Следует отметить ряд хостов, которые «очистились» от плохого содержимого, а также усилия правоохранительных органов, которые сыграли в этом процессе немаловажную роль.

Несмотря на все сказанное выше, самый плохой хост #1 по прежнему относится к провайдеру из США, и хотя он не новичок в списке Топ 10, данный хост впервые попадает на ведущую позицию. Теперь #1 место занимает AS33626 Oversee.net благодаря размещению плохих URL, вредоносного ПО, серверов ботнетов Zeus и прочих угроз. Oversee.net также продает доменные имена и управляет другими сервисами, связанными с обслуживанием доменов. Согласно пресс-релизам за последнее время Oversee сократила 13% персонала с целью 'перераспределения трудовых ресурсов', а также выступила ответчиком в суде по искам от бывшего сотрудника и клиента.

Чтобы поддержать хосты, предпринимающие усилия для «очистки» своих серверов, отчет Топ 50 по-прежнему содержит раздел «Улучшенные хосты». Лучших в данной категории — AS38333 Symbio Networks и AS5605 Netuse можно поздравить. Также следует отметить бывший плохой хост #1 и регулярный участник рейтинга Топ 10 в предыдущих кварталах, AS29073 Ecatel, который полностью покинул список TOP 50 в этом квартале. Мы надеемся, что больше не увидим Ecatel в нашем рейтинге, причем по самым хорошим причинам!

Не удивительно, что плохой хост #2, AS47583 Hosting-Media, был также отмечен как #1 в категории «Эксплойт-серверы», которую мы считаем наиболее важной в анализе распространения вредоносного ПО, фишинга и другого плохого контента.

Хосты и корпоративные сети не всегда добровольно размещают на своих серверах вредоносный контент. Злонамеренное ПО может распространяться серверами, захваченными и зомбированными в результате взлома и компрометации. Такие сети были отмечены как «Эксплойт-серверы», они могут быть использованы для дальнейшего распространения вредоносного контента и нежелательных материалов под маской других активностей, что затрудняет детектирование угроз.

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 AC для использования в BGP маршрутизации. Номера AC 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)*