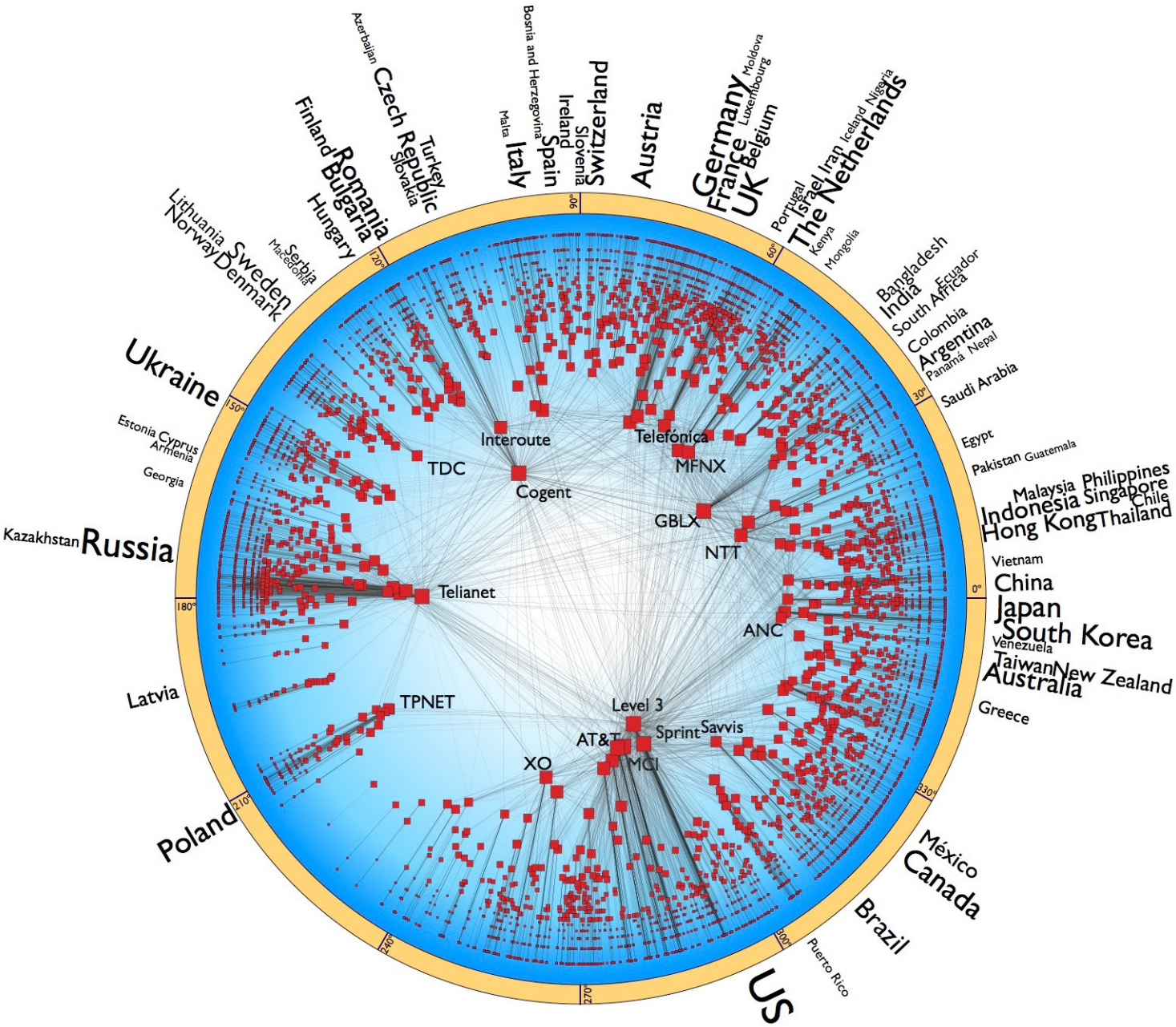
Мировая серия «Компьютерные преступления»

Топ 50 «Самые зараженные хосты и сети»
Отчет по итогам второго квартала 2011 года



SITEVET

HOST exploit

GROUP IB

Оглавление

Топ 50

Серия «Компьютерные преступления»

Самые зараженные хосты и сети

Backing from

nominet trust

www.nominettrust.org.uk

Редактор

- Jart Armin

Рецензенты

- Dr. Bob Bruen
- Raoul Chiesa
- Alexander Fominenkov
- Bogdan Vovchenko
- Sergey Nikitin
- Alexander Kalinin
- Vesta Matveeva
- Valeriy Baulin

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
- MalwareURL
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- StopBadware
- SudoSecure
- Sunbelt
- Team Cymru
- UCE Protect

Front page illustration: Bogu ñ á , M. et al. Sustaining the Internet with hyperbolic mapping. Nat. Commun. 1:62 doi: 10.1038 / ncomms1063 (2010).

Самые зараженные хосты и сети

Утечки информации

В последнее время внимание мировой прессы привлекли взломы популярных сайтов, ответственность за которые брали на себя хакерские группы Anonymous или LulzSec. Атаки на различные интернет-ресурсы приобретают все больший размах. Так, в период с апреля по июнь 2011 года была зафиксирована компрометация 450 000 сайтов, тогда как за весь 2010 год отмечалось 1,5 млн. взломов.

За последний квартал хакеры организовали несколько впечатляющих хищений информации из информационных систем таких корпораций, как Sony, Citybank, RSA и других. Каким же образом, проникнув в корпоративную сеть, злоумышленники извлекают всю необходимую им информацию за такое короткое время? И как им при этом удается оставаться незамеченными?

Ответ на первый вопрос может кого-то удивить, но тем не менее, после удачного проникновения в систему, хищение данных может продолжаться недели и даже годы. В исследовании, проведенном SpiderLabs компании Trustwave в 2009 г. на выборке из 218 нарушений по всему миру, установлено, что средний срок между взломом и его обнаружением составлял 156 дней.

И это еще относительно короткий срок в сравнении, например, с обнаруженной компанией McAfee целенаправленной угрозой (Advanced Persistent Threat), под названием «Ночь Дракона». Данная атака продолжалась на протяжении четырех лет. Другой пример — хищение данных из Государственного департамента США для WikiLeaks, которое совершалось в течение нескольких месяцев.

Вопреки распространенному мнению, хакеры не действуют, как налетчики, руководствуясь принципом «разгромить и забрать». Злоумышленники могут и затаиться, чтобы избежать обнаружения, выжидая лучшего времени для хищения всего объема информации, или, наоборот, извлекать небольшие фрагменты данных в течение длительного периода времени.

До того, как похитить данные из системы, злоумышленники могут хранить их в защищенных паролем RAR, ZIP, CAB архивах, которые могут долго оставаться незамеченным, пока занимаемый ими объем дискового пространства не становится опасной большим для обнаружения. Обычно это порядка 1 процента.

По сообщениям Trustwave, использование одного и того же способа удаленного доступа при проникновении в систему и для хищения данных было замечено всего в 38 случаях. В случае применения вредоносного ПО, такого как клавиатурные шпионы, в основном используются уязвимости FTP и электронной почты. Это, например, установка ложного SMTP-сервера непосредственно на скомпрометированной системе.

Самый распространенный метод скрытного хищения данных — это атака через DNS (систему доменных имен). Этот метод может использоваться даже в системах, неподключенных к публичным сетям, в случае разрешения запросов доменных имен за пределы доверенной сети с помощью цепочки внутренних и внешних DNS-серверов.

Хотя большая часть сетевой активности серверов журналируется, именно сервер баз данных зачастую оказывается без внимания, так как в основном журналирование осуществляется на сервере приложений и преимущественно входящих соединений. Дело в том, что именно исходящим DNS-запросам, как никаким другим, разрешен доступ к произвольным хостам в сети Интернет. Даже тогда, когда брандмауэры настроены так, чтобы предотвратить непосредственную отправку пакетов в Интернет с сервера баз данных, хакеры могут отправлять DNS-запросы с внутреннего DNS-сервера с использованием SQL-инъекций.

Для передачи данных злоумышленники также могут применять временные задержки между отсылаемыми пакетами. Кроме того, они активно используют стеганографию, при которой похищаемая информация скрывается в графических, pdf и мультимедиа файлах, а также шпионское программное обеспечение и — если есть возможность получить физический доступ в помещение — скрытые аппаратные устройства.

В конечном счете, хакеры используют наши самые большие слабости против нас, анализируя исходящий траффик, к контролю над которым в большинстве организаций уделяется мало внимания. К тому же предприятия, как правило, сами не представляют уровень критичности данных, которые они обрабатывают, и не располагают комплексными знаниями о структуре потоков внутри собственных систем.

Вредоносное ПО Conficker

Заметных успехов в борьбе с киберпреступностью добилась Служба безопасности Украины (СБУ). Она обнародовала подробности участия в международной операции, в которой были задействованы спецслужбы 10 стран. Операция была направлена на прекращение противоправной деятельности злоумышленников, которые, как утверждается, использовали зараженные вирусом Conficker компьютеры с целью несанкционированного доступа к банковским счетам по всему миру.

ФБР ранее объявило, что деятельность преступной группы, использовавшей сложную схему с использованием вредоносного ПО, была прекращена в результате совместной операции нескольких стран. Служба безопасности Украины сообщает, что ее сотрудники провели обыски в 19 организациях, в ходе которых было изъято более 74 единиц компьютерной техники, около 300 единиц электронных носителей, документы и денежные средства. Заявляется, что злоумышленники похитили более 72 млн долларов США путем мошенничества в системах интернет-банкинга. Деньги были обналичены через международные платежные системы и счета других банков.

Следователи СБУ допросили 16 человек в Киеве, Харькове и Луганске. Предполагалось, что они организовали и координировали деятельность международной преступной группы, которая действовала под видом легальной коммерческой организации.

В свою очередь, правоохранительные органы США, Великобритании, Нидерландов, Франции, Германии, Кипра и Латвии провели более 30 обысков. При этом в Латвии были арестованы два подозреваемых. Так же Служба безопасности Украины сообщает, что более чем 40 банковских счетов были заморожены в Латвии и на Кипре.

Взлом по SSH

IB мае 2011 года была совершена серьезная кибератака против ассоциации Euro-IX.

Злоумышленники использовали уязвимость в процедуре входа через протокол SSH с применением утилит “ssh_decoder” и “bfssh”.

Атака была сорвана благодаря проактивной системе защиты сервера. Дальнейший анализ показал, что для согласование атак использовался абузоустойчивый хостинг secretsline.biz — специальный анонимный VPN-сервис, который в настоящее время располагается на следующих автономных системах:

- AS24940 HETZNER (DE)
- AS3.135 INTERFRAME (32 bit ASN)
- AS35017 SWIFTWAY (NL)

Защита цепочек поставок компьютерного оборудования и ПО

Аналитический центр EastWest Institute (EWI) и Европейское агентство сетевой и информационной безопасности (ENISA) считают, что обеспечение целостности цепочек поставок входит в пятерку самых значимых исследовательских задач. Хотя признается, что эта тема крайне сложна для изучения.

Тем не менее, в документах, представленных китайскими исследователями на недавнем саммите EWI в Лондоне, предлагаются практические и инновационные решения данной проблемы.

Авторы, Сяофэн Цю (Xiaofeng Qiu) из Пекинского университета и Лян Чжао (Liang Zhao) из NSFocus, считают, что существующие стандарты в области цепочек поставок компьютерного оборудования и ПО не состоятельны и должны обязательно включать в себя тестирование на уязвимости. Слабость любого звена цепочки может привести к инъекции вредоносного кода в программные или аппаратные компоненты, прежде чем они доберутся до места назначения. Целостность цепочек поставок компьютерного оборудования и ПО является, таким образом, необходимым условием для обеспечения безопасности ИТ.

В своем исследовании ученые сфокусировались в частности на случаях, когда тестирование на уязвимости не проводилось, вследствие чего не были выявлены скрытые каналы — места в цепочке поставок, когда информация передается между процессами там, где этого не должно происходить.

Слово редактора

Стандартизация данных — новых подход к снижению ложных срабатываний

Темой данного отчета является количественная оценка уровня зараженности хостов по всему миру. Она позволяет составить актуальные «черные списки», которые являются эффективным инструментом в руках конечных пользователей и организаций для обнаружения злоумышленников.

Однако, при использовании «черных списков», предоставляемых сторонними специализированными компаниями, всегда присутствует неизбежная задержка в ответной реакции на новые угрозы. По этой причине мы рекомендуем использовать «черные списки» только как вспомогательный инструмент по обнаружению зловредной активности.

«Черные списки», составленные различными организациями, зачастую компонуются вручную небольшой группой исследователей-аналитиков. Результаты данной работы являются хорошим дополнением при использовании автоматизированных систем обнаружения атак таких, как IPS, IDS и межсетевые экраны.

За последние несколько лет подобные списки получили довольно широкое распространение: от нескольких до сотен регулярно используемых сервисов, преимущественно специализирующихся на отдельных категориях вредоносной активности. Одной из проблем, кроющейся за столь быстрым распространением таких сервисов, является отсутствие кооперации и единообразия между используемыми списками. Как результат, «черные списки» различных сообществ более склонны к соперничеству, чем взаимодействию. Причем в большинстве случаев это не является преднамеренной стратегией, а происходит из-за сложностей в обмене информацией. Единые стандарты обмена подобной информацией отсутствуют и, как следствие, разные сообщества используют свои собственные форматы предоставления данных (за исключением случаев, когда «черные списки» ведутся с целью добавления сигнатур в межсетевые экраны и средства обнаружения вторжений, однако это опять не облегчает задачу обмена информацией, так как является конечным форматом для конкретной системы).

Факторы, описанные выше, приводят к большому числу ложных срабатываний в различных «черных списках». Во многих из них процедура обработки таких срабатываний отсутствует. Те, в которых она все же есть, требуют определенного времени, чтобы обработать запись и перенести ее в белый список. А по причине отсутствия единых стандартов опять же не существует унифицированного метода массовой обработки ложных срабатываний.

Наличие подобного метода может обеспечить хостам и регистраторам обратную связь с компаниями, составляющими «черные списки». Это помогло бы улучшить качество списков, посредством исключения ложных записей, которые отвлекают от реальных проблем. «Черные списки» будут располагать более точными данными для анализа, а также возможностью улучшить методологию, в то же самое время конечные пользователи и организации получают корректный список для фильтрации.

Рассмотрим в качестве примера недавно запущенный сервис от Google — Google's Safe Browsing list. Этот замечательный сервис помогает защитить конечных пользователей от вредоносных и подозрительных вебсайтов посредством блокирования их на уровне браузера (используется по умолчанию в Google Chrome и Mozilla Firefox). Работа с Google до недавнего времени основывалась на поиске ложных записей в их фишинг-листе. В итоге, более 80% записей, касаемо AS21740 eNom, оказались ложными.

Компания уже начала вносить изменения, которые позволят устранить проблему ложных срабатываний и сфокусировать внимание на обнаружении действительно фишинговых и вредоносных вебсайтов.

К счастью, Google обладает достаточным количеством ресурсов для улучшения собственной методологии. Но для небольших организаций, издающих собственные «черные списки», ситуация обстоит иначе. По этой причине мы работаем над стандартом, который позволит обеспечить взаимодействие между разными сообществами и установить единообразие между различными «черными списками».

Если Вы заинтересованы в получении дополнительной информации или хотите принять участие в написании данного стандарта, пишите нам или нашими партнерам в Российской Федерации.

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

Jart Armin

Часто задаваемые вопросы

В 2009 году мы разработали Индекс HE — 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 HE 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 HE 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 HE 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.

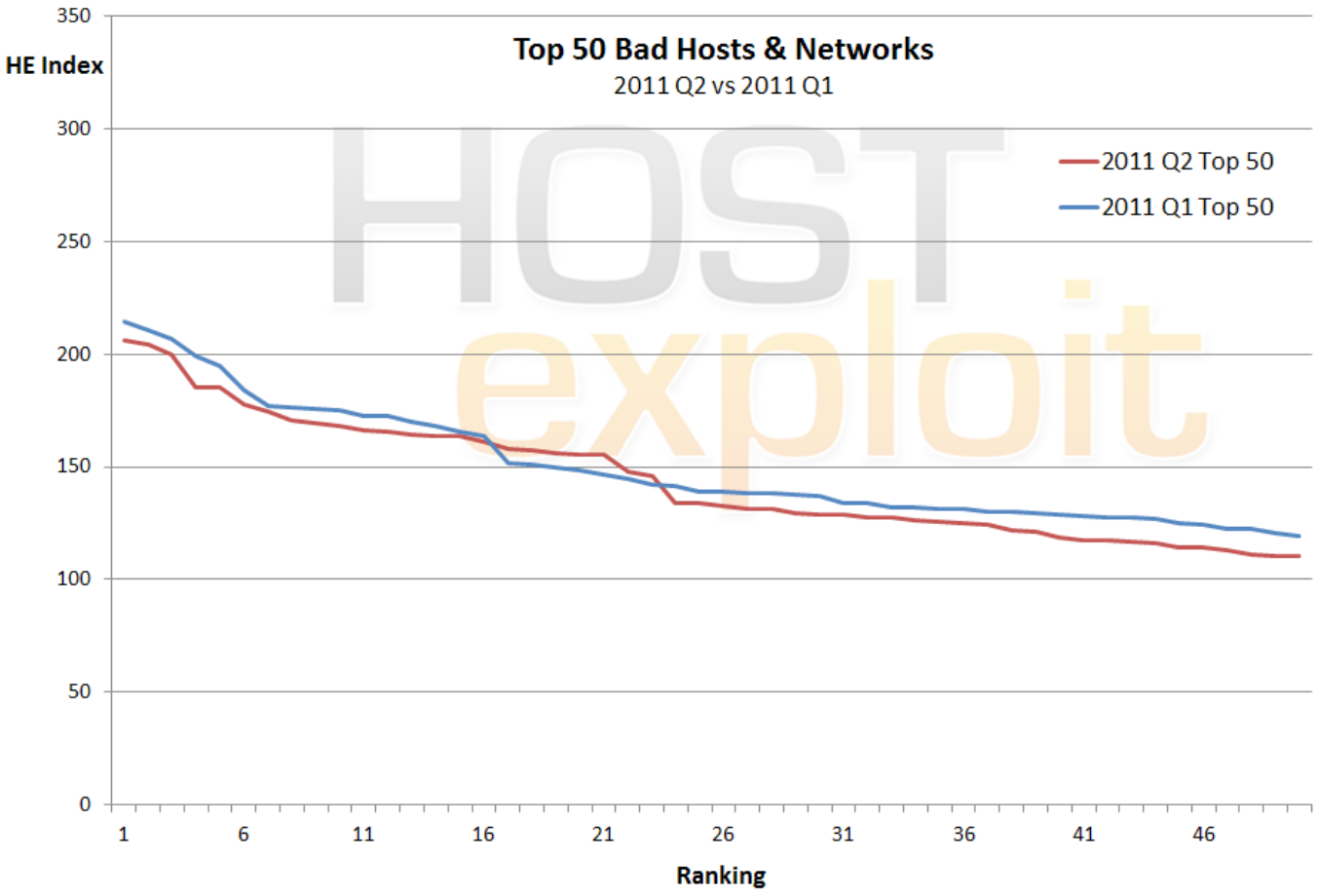
Обратная связь приветствуется!

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

3. Топ 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	206.0	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	39,680
▶ 2	204.6	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
▲ 3	200.1	10297	ENET-2 - eNET Inc.	US	90,880
▼ 4	185.3	41947	WEBALTA-AS OAO Webalta	RU	16,128
▲ 5	185.2	21788	NOC - Network Operations Center Inc.	US	282,624
▶ 6	177.8	36408	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	US	37,376
▲ 7	174.2	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▲ 8	170.9	36167	NETRIPLEX01 - NETRIPLEX LLC	US	46,080
▲ 9	169.4	46844	ST-BGP - SHARKTECH INTERNET SERVICES	US	75,520
▲ 10	168.3	9809	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	CN	11,008
▲ 11	166.3	28753	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt e. K.)	DE	104,960
▼ 12	165.3	16138	INTERIAPL INTERIA.PL SA	PL	4,096
▼ 13	164.1	45899	VNPT-AS-VN VNPT Corp	VN	2,024,704
▲ 14	163.9	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,548,800
▲ 15	163.7	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,640
▼ 16	161.1	6851	BKCNET "SIA" IZZI	LV	49,152
▲ 17	157.8	33774	DJAWEB	DZ	67,840
▼ 18	157.0	24940	HETZNER-AS Hetzner Online AG RZ	DE	502,784
▲ 19	156.1	32475	SINGLEHOP-INC - SingleHop	US	218,624
▲ 20	155.4	36057	WEBAIR-AMS Webair Internet Development Inc	US	25,344
▼ 21	155.3	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	109,796,608
▼ 22	148.0	16276	OVH OVH	FR	546,816
▶ 23	145.8	13727	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024
▲ 24	133.8	50693	KONSING-GROUP Konsing group doo	SP	2,048
▼ 25	133.6	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	73,728
▲ 26	132.5	22489	CASTLE-ACCESS - Castle Access Inc	US	48,384
▲ 27	131.2	8560	ONEANDONE-AS 1&1 Internet AG	DE	357,888
▲ 28	131.0	26496	PAH-INC - GoDaddy.com, Inc.	US	1,135,616
▼ 29	129.5	6697	BELPAK-AS BELPAK	BY	747,520
▲ 30	128.9	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	887,552
▲ 31	128.5	40824	WZCOM-US - WZ Communications Inc.	US	8,960
▲ 32	127.3	37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology	CN	4,096
▲ 33	127.2	39150	TRANSIT-TELECOM-AS Tranzit Telecom LTD	RU	5,376
▲ 34	126.2	6400	CompaÃ±Ãa Dominicana de TelÃ©fonos, C. por A. - CODETEL	DO	390,912
▲ 35	125.6	15169	GOOGLE - Google Inc.	US	284,160
▲ 36	125.0	31147	INLINE-AS Inline Internet Online Dienste GmbH	DE	9,728
▲ 37	124.2	9050	RTD ROMTELECOM S.A	RO	1,645,824
▲ 38	122.0	11798	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	235,520
▲ 39	121.1	35908	VPLSNET - VPLS Inc. d	US	714,240
▲ 40	118.7	16265	LEASEWEB LEASEWEB AS	NL	276,736
▼ 41	117.2	29182	ISPSYSTEM-AS ISPsystem Autonomous System	RU	35,840
▲ 42	117.2	23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone	CN	116,256
▼ 43	116.6	49981	WORLDSTREAM WORLDSTREAM AS	NL	11,520
▼ 44	116.1	30058	FDCSERVERS - FDCservers.net	US	242,432
▼ 45	114.4	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,810,432
▲ 46	113.9	30083	SERVER4YOU - Hosting Solutions International, Inc.	US	20,480
▲ 47	113.2	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San	TR	13,056
▲ 48	111.0	14585	CIFNET - CIFNet, Inc.	US	7,680
▲ 49	110.3	51306	UAIP-AS PAN-SAM Ltd.	UA	2,048
▼ 50	110.2	32181	ASN-GIGENET - GigeNET	US	42,240

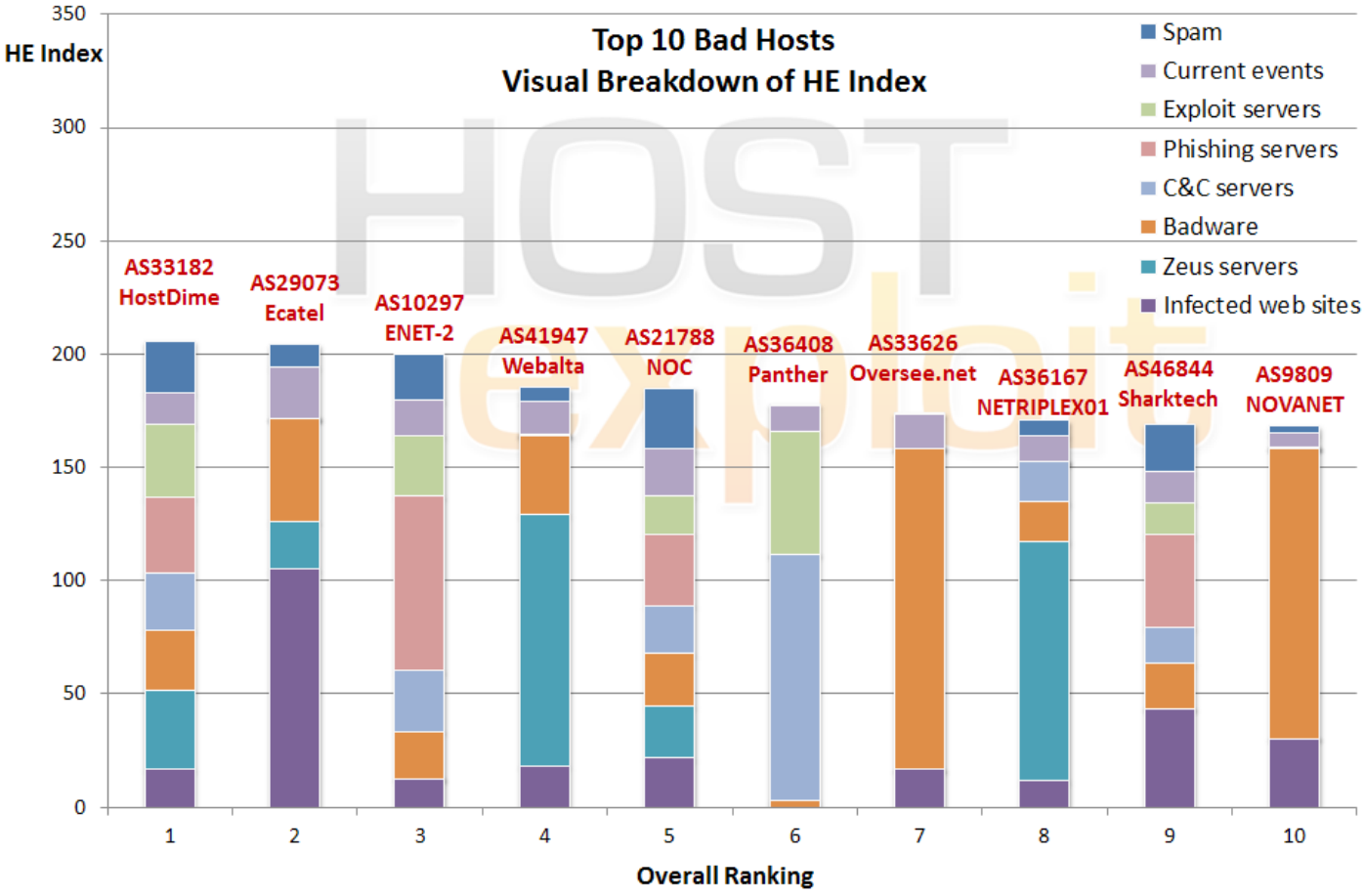
Сравнение первого и второго квартала 2011 года



Сравнение Топ 50 «Самые зараженные хосты» с марта по июнь 2011 года.

В целом, в рамках Топ 50 уровень зараженности практически не изменялся в течение квартала.

Топ 10. График распределения Индекса HE



Приведенный выше график распределения Индекса HE в списке Топ 10 «Самые зараженные хосты» наглядно демонстрирует две вещи.

Во-первых, согласно приведенному графику распределения Индекса HE в различных категориях среди представленных хостов нельзя выделить один, который бы явно доминировал над другими по уровню зараженности. Данное заключение позволяет сделать вывод о том, что Индекс предоставляет сбалансированную независимую оценку.

Во-вторых, график демонстрирует распределение Индекса HE для каждой автономной системы в Топ 10, по которому можно наглядно оценить степень той или иной злонамеренной активности для каждой АС.

Например, AS33182 HostDime (US) занимает первое место из-за своего широкого спектра зловредной активности и объектов, включающих в себя спам, эксплоит-серверы, фишинговые сервера и zeus-серверы, а также некоторое количество серверов управления ботнетами, вредоносного ПО и зараженных веб-сайтов.

Автономная система AS41947 Webalta (RU) опустилась на четвертое место с первого в прошлом квартальном отчете.

Новое за квартал

6.1. Обзор

	Previous Quarter - Q1 2011			Current Quarter - Q2 2011		
	ASN	Name	Country	ASN	Name	Country
#1	41947	Webalta	RU	33182	HostDime	US
#2	29073	Ecatel	NL	29073	Ecatel	NL
#3	16138	Interia.pl	PL	10297	eNET	US
#1 for Spam	45899	VNPT	VN	33774	DJAWEB	DZ
#1 for Botnets	36408	Panther Express / CDNetworks	US	36408	Panther Express / CDNetworks	US
#1 for Zeus Botnet	49469	Sa Nova Telecom	RO	41947	Webalta	RU
#1 for Phishing	10297	ENET-2 - eNET Inc.	US	10297	ENET-2 - eNET Inc.	US
#1 for Exploit Servers	21607	DeployLinux	US	14585	CIFNet Inc.	US
#1 for Badware	33626	Oversee.net	US	33626	Oversee.net	US
#1 for Infected Sites	6851	BKCNET "SIA" IZZI	LV	29073	Ecatel	NL
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

6.2. Топ 10. Вновь зарегистрированные хосты

HE Rank	HE Index	AS number	AS name	Country	# of IPs
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

Примечание: к концу второго квартала 2011 года было зарегистрировано 38030 автономных систем, что на 759 больше, чем на конец первого квартала 2011 года.

6.3. Вылеченные хосты

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-84.2%	62	112.3	2,787	17.8	47764	NETBRIDGE-AS... LLC... Mail.Ru	RU	12,032
-64.3%	59	113.0	1,019	40.4	9280	CIA-AS connect infobahn australia (CIA)	AU	8,704
-62.5%	60	112.7	910	42.3	21607	DEPLOYLINUX - DeployLinux Consulting	US	512
-60.4%	34	131.9	539	52.3	31133	MF-MGSM-AS OJSC MegaFon Network	RU	16,128
-57.0%	81	102.5	831	44.1	13301	UNITEDCOLO-AS... unitedcolo.de	DE	67,072
-56.8%	54	116.1	600	50.2	23860	ALLIANCE-GATEWAY-AS-AP...	IN	16,384
-55.2%	50	119.6	514	53.6	40634	FIRSTLOOK-COM - FirstLook, Inc.	US	512
-54.6%	53	117.0	523	53.1	27715	LocaWeb Ltda	BR	83,200
-53.1%	159	82.2	1,094	38.6	34449	MORDOVIA-AS... Mordovian Republic...	RU	63,488
-52.4%	22	144.6	225	68.8	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,624

Многие формы вредоносного ПО могут быть неразрывно связаны между собой, что является неразрешимой проблемой для некоторых хостов. Тем не менее, мы хотели бы выделить ряд автономных систем, представленных в таблице выше, которым удалось резко сократить уровень зараженности всего за три месяца с момента публикации нашего отчета за первый квартал 2011 года.

Эти 10 хостов существенно отличаются размерами, расположением, видом деятельности и типом вредоносности, которую удалось вылечить. Это показывает, что при любых обстоятельствах есть возможность улучшить ситуацию, применив соответствующие усилия и нестандартный подход.

Для справки:

AS47764 Netbridge – автономная система, в которой располагается популярный почтовый сервис Mail.ru — сместился с показателя #62на #2787 (процент снижения уровня зараженности — 84%).

A21607 DeployLinux — будучи долгое время в рейтинге Топ 50 — существенно улучшила свое положение, снизив уровень зараженности на 62%.

6.4. Хосты, состояние которых ухудшилось

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
5,370.4%	22,632	1.5	112	84.6	49130	ARNET-AS SC ArNet Connection SRL	RO	768
4,870.1%	20,057	1.5	159	76.9	16125	DC-AS UAB Duomenu Centras	LT	4,608
540.1%	3,794	13.3	109	85.2	50465	IQHOST IQHost Ltd	RU	1,024
289.8%	1,978	27.1	62	105.5	50244	ITELECOM Pixel View SRL	RO	7,936
125.6%	1,413	35.4	131	79.9	42244	ESERVER eServer.ru - hosting operator	RU	5,120
82.0%	756	49.4	95	90.0	48587	NET-0X2A-AS Zharkov Mukola...	UA	1,024
68.4%	585	55.5	86	93.6	44112	SWEB-AS SpaceWeb JSC	RU	3,072
48.7%	553	56.7	113	84.3	8001	NET-ACCESS-CORP - Net Access Corp...	US	503,040
40.2%	130	88.6	37	124.2	9050	RTD ROMTELECOM S.A	RO	1,645,824
35.9%	109	91.9	36	125.0	31147	INLINE-AS Inline Internet Online...	DE	9,728

В данном разделе представлены хосты, уровень зараженности которых существенно увеличился по сравнению с прошлым кварталом. По этой причине в данном разделе не представлены вновь зарегистрированные зараженные хосты.

Для просмотра вновь зарегистрированных хостов вы можете перейти в раздел 6.2.

В этом квартале стоит выделить два «выдающихся» хоста, с чрезвычайно сильным увеличением уровня зараженности.

Во-первых, это AS49130 ArNet (RO), которая сейчас #112 с всего лишь 768 IP-адресами.

Во-вторых, это AS16125 Duomenu Centras (LT), которая поднялась на #159 позицию.

Стоит отметить, что в предыдущем квартале оба хоста были довольно непримечательными.

Автономные системы IQHost, ITelecom, Eserver и SpaceWeb также значительно увеличили уровень зараженности за прошедший квартал.

Сходством всех представленных автономных систем является малое количество выделенных IP-адресов, что характерно для небольших серверов, используемых киберпреступниками.

Анализ по странам

Hosts in Top 50	Country	Total IPs within Top 50	Total Index	Average Index	Average Indexes by Category							
					Infected web sites	Zeus servers	Badware	C&C servers	Phishing servers	Exploit servers	Current events	Spam
23	UNITED STATES	6,118,400	3,397.0	147.7	167.8	94.5	192.6	215.7	195.0	261.5	130.4	55.2
4	GERMANY	975,360	579.5	144.9	270.3	191.9	149.9	132.4	112.0	188.8	118.7	70.9
4	CHINA	109,927,968	568.0	142.0	166.5	39.0	328.5	217.6	34.4	169.4	105.0	64.4
3	NETHERLANDS	301,824	439.9	146.6	452.8	172.1	218.1	57.1	0.1	53.9	151.5	55.3
3	RUSSIA	57,344	429.8	143.3	450.6	371.3	191.2	0.2	0.1	0.5	125.0	19.5
1	POLAND	4,096	165.3	165.3	107.4	0.2	275.8	0.3	0.2	0.7	949.5	3.2
1	VIETNAM	2,024,704	164.1	164.1	100.1	0.0	35.2	0.0	0.0	0.0	100.1	587.7
1	LATVIA	49,152	161.1	161.1	871.4	0.1	198.8	0.1	0.1	0.2	185.3	36.9
1	ALGERIA	67,840	157.8	157.8	64.3	0.0	53.1	0.1	0.1	0.2	0.0	616.1
1	FRANCE	546,816	148.0	148.0	161.5	140.8	142.1	144.6	262.0	210.6	119.2	106.2
1	CANADA	1,024	145.8	145.8	184.8	230.7	553.2	0.4	0.2	0.8	101.6	3.7
1	SERBIA	2,048	133.8	133.8	0.5	0.2	0.4	0.4	0.2	0.8	0.1	578.8
1	BELARUS	747,520	129.5	129.5	103.0	0.0	100.7	107.4	0.0	115.0	100.1	300.6
1	DOMINICAN REP.	390,912	126.2	126.2	0.0	0.0	0.0	0.0	0.0	0.0	27.3	533.0
1	ROMANIA	1,645,824	124.2	124.2	100.1	0.0	100.3	0.0	0.0	0.0	100.0	371.3
1	INDIA	1,810,432	114.4	114.4	100.2	0.0	100.1	0.0	0.0	0.0	100.0	329.0
1	TURKEY	13,056	113.2	113.2	32.7	0.1	116.2	202.5	0.2	557.6	100.9	59.0
1	UKRAINE	2,048	110.3	110.3	701.4	0.2	103.9	0.4	0.2	0.8	105.2	4.7

«Чистые» хосты

HE Rank	HE Index	AS number	AS name	Country	# of IPs
36,515	**0.28**	**34744**	GVM S.C. GVM SISTEM 2003 S.R.L.	**RO**	482,816
36,488	**0.30**	**5583**	ORANGE-BUSINESS-SERVICES-BENELUX Orange...	**FR**	343,040
36,436	**0.34**	**3764**	IA-HOU-AS - Internet America, Inc.	**US**	201,216
36,353	**0.39**	**19855**	ASN-MASERGY-US Masergy US Autonomous System	**US**	132,096
36,207	**0.47**	**4004**	ORANGE-BUSINESS-SERVICES-UK Orange...	**US**	83,968
36,205	**0.47**	**17229**	ATT-CERFNET-BLOCK - AT&T Enhanced Network Services	**US**	83,456
36,190	**0.48**	**9476**	INTRAPOWER-AS-AP IntraPower Pty. Ltd.	**AU**	78,080
36,154	**0.49**	**41230**	ASK4 Ask4 Limited	**UK**	73,728
36,125	**0.51**	**18705**	RIMBLACKBERRY - Research In Motion Limited	**CA**	67,072
35,977	**0.57**	**3112**	OARNET-AS-1 - OARnet	**OH**	220,160

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.

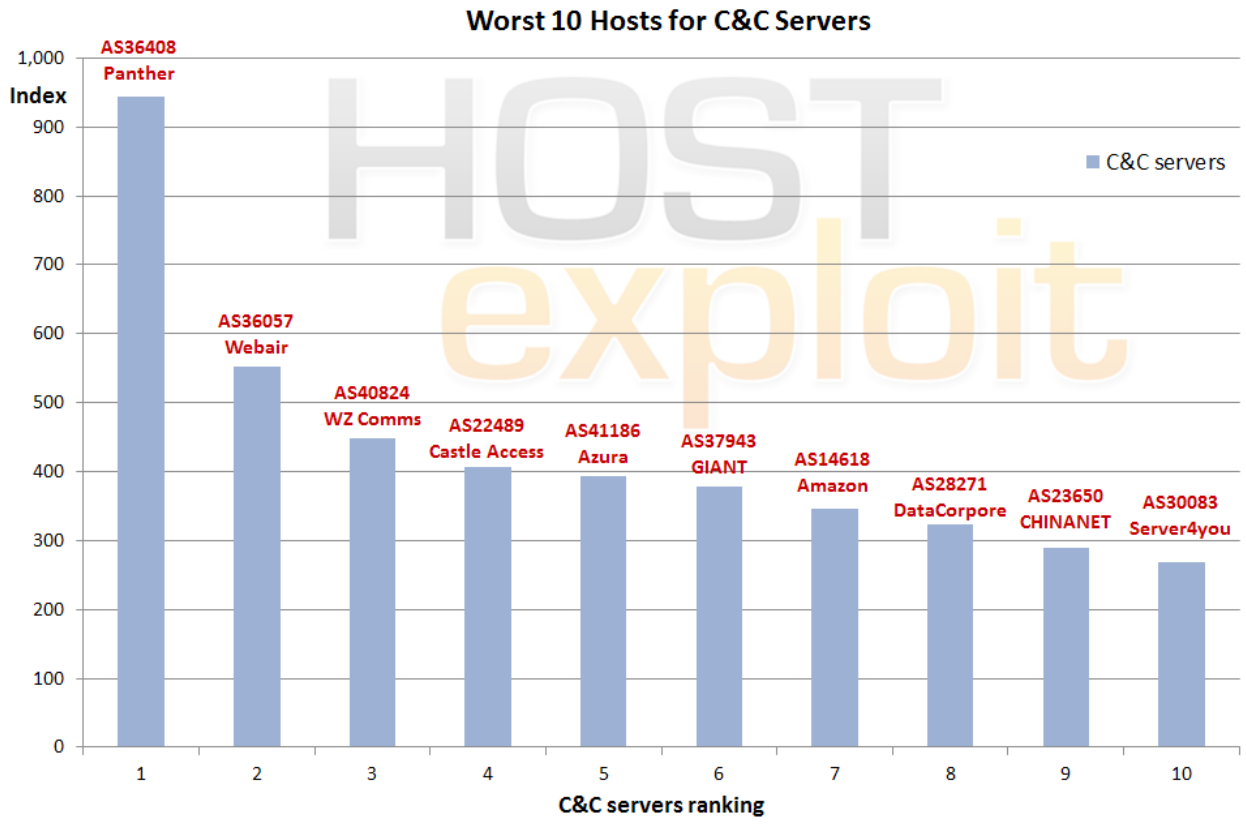
Опасные хосты по категориям

9.1.1. Серверы управления ботнетами

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
6	177.8	**36408**	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	**US**	37,376	**943.8**
20	155.4	**36057**	WEBAIR-AMS Webair Internet Development Inc	**US**	25,344	**552.7**
31	128.5	**40824**	WZCOM-US - WZ Communications Inc.	**US**	8,960	**449.2**
26	132.5	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	48,384	**406.5**
94	91.3	**41186**	ISPFR-AS AZURA NETWORKS	**FR**	2,816	**394.0**
32	127.3	**37943**	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology...	**CN**	4,096	**378.7**
52	110.0	**14618**	AMAZON-AES - Amazon.com, Inc.	**US**	528,384	**345.8**
72	101.0	**28271**	DataCorpore ServiÃ§os e RepresentaÃ§Ãµes	**BR**	10,240	**323.3**
42	117.2	**23650**	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province...	**CN**	116,256	**290.3**
46	113.9	**30083**	SERVER4YOU - Hosting Solutions International, Inc.	**US**	20,480	**268.4**

Как и в предыдущих отчетах, присутствует тенденция смещения серверов управления ботнетами в сторону более крупных хостов. Наши данные полностью совпадают с показаниями сообщества по борьбе с киберпреступностью Shadowserver.

Положение США не изменилось, как и в прошлом квартале им принадлежит 6 из 10 позиций.

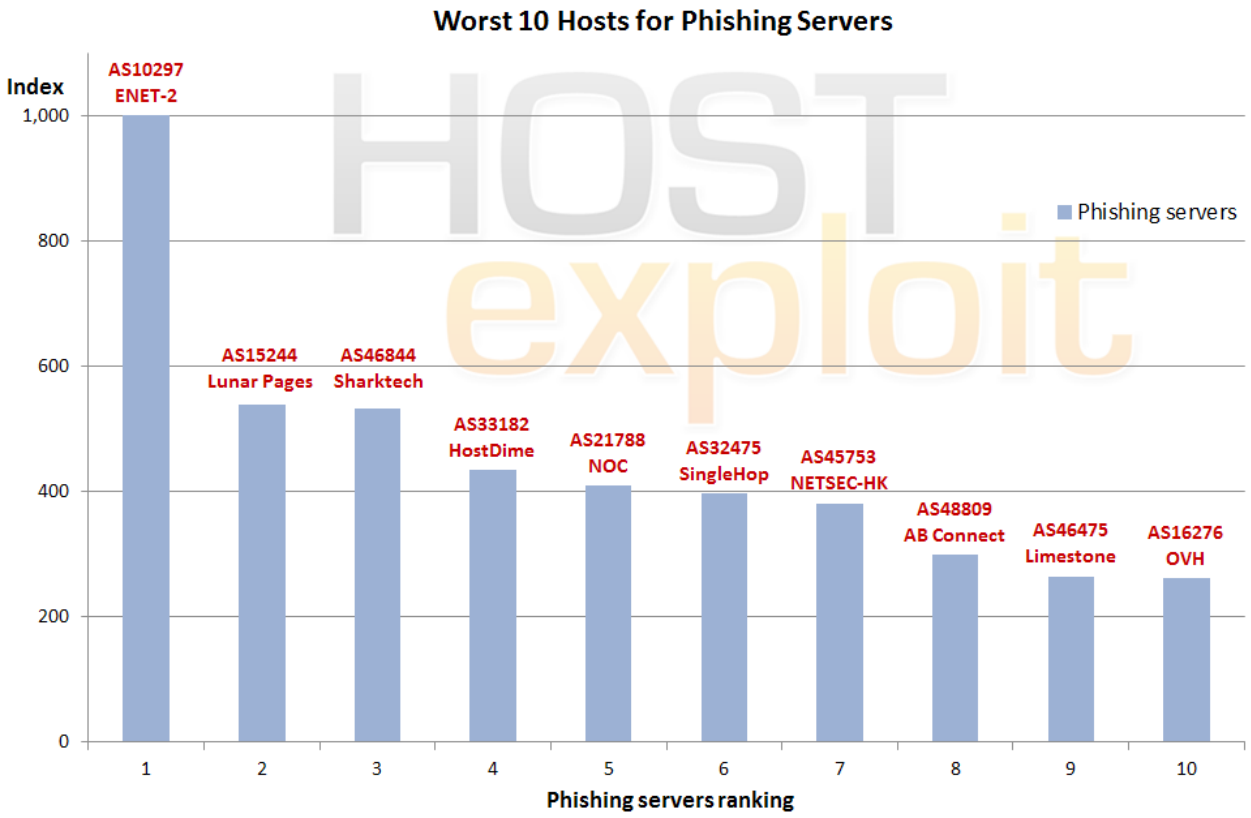


9.1.2. Фишинговые сервера

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	200.1	**10297**	ENET-2 - eNET Inc.	**US**	90,880	**1000.0**
15	163.7	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	48,640	**539.7**
9	169.4	**46844**	ST-BGP - SHARKTECH INTERNET SERVICES	**US**	75,520	**533.2**
1	206.0	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	39,680	**434.0**
5	185.2	**21788**	NOC - Network Operations Center Inc.	**US**	282,624	**410.4**
19	156.1	**32475**	SINGLEHOP-INC - SingleHop	**US**	218,624	**398.0**
89	93.4	**45753**	--No Registry Entry--	**HK**	113,408	**381.8**
435	56.8	**48809**	ABCONNECT AB CONNECT	**FR**	4,096	**299.2**
25	133.6	**46475**	LIMESTONENETWORKS - Limestone Networks, Inc.	**US**	73,728	**265.3**
22	148.0	**16276**	OVH OVH	**FR**	546,816	**262.0**

Резкое увеличение количества западных стран в Топ 10 фишинговых ресурсов можно объяснить традиционным доверием пользователей к сайтам, зарегистрированным в этом регионе. Фишинг по-прежнему является причиной для беспокойства банков и крупных корпораций. Результаты нашего исследования показывают, что 6 фишинг-хостов из списка Топ 10 находятся в США.

Вредоносное ПО может находиться на вебсайте корпорации и загружаться через выполнение межсайтовых сценариев или через перенаправление. Нахождение этого ПО на легальных сайтах западных компаний снижает уровень бдительности как клиентов, так и партнеров.



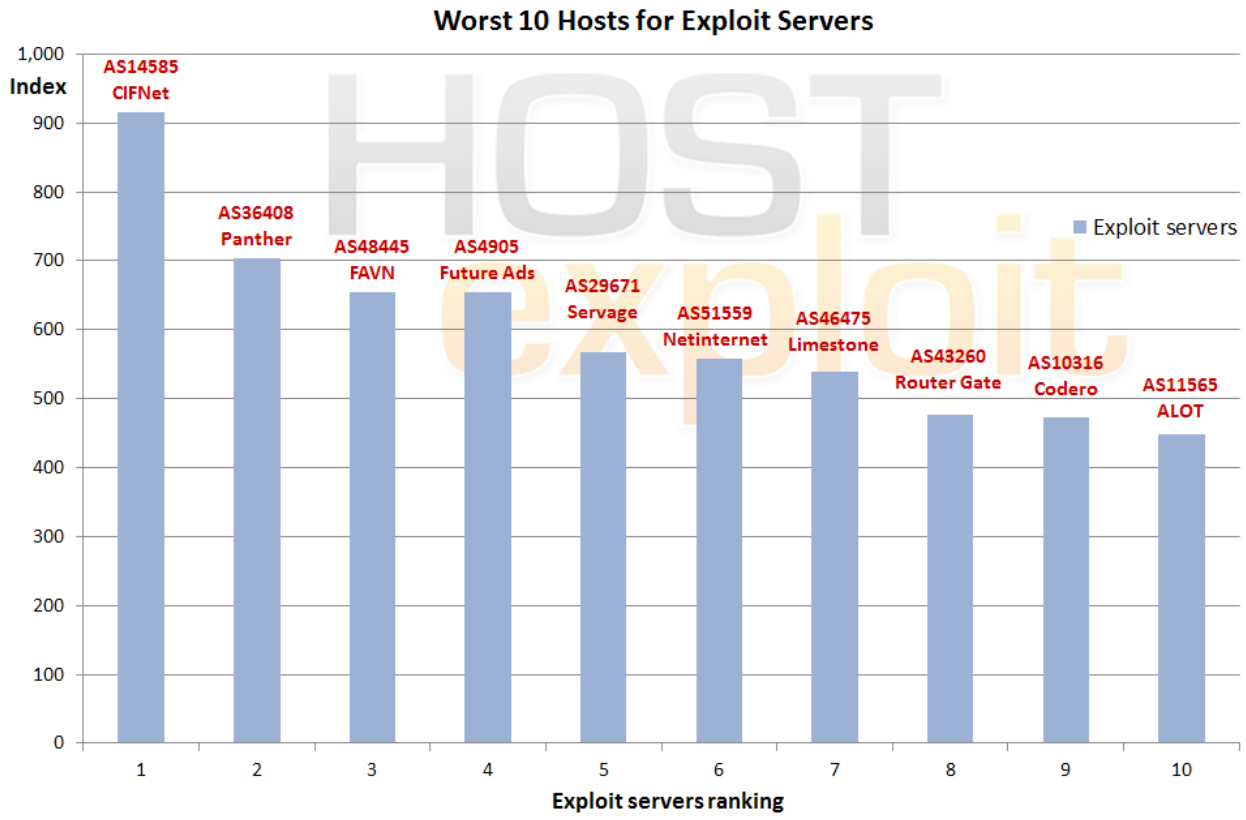
9.1.3. Эксплоит-серверы

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
48	111.0	**14585**	CIFNET - CIFNet, Inc.	**US**	7,680	**916.2**
6	177.8	**36408**	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	**US**	37,376	**703.1**
92	92.3	**48445**	FAVN Favorit Network SL	**ES**	256	**655.1**
518	53.4	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**655.1**
53	109.7	**29671**	SERVAGE Servage GmbH	**DE**	12,288	**568.2**
47	113.2	**51559**	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon...	**TR**	13,056	**557.6**
64	104.9	**22822**	LLNW - Limelight Networks, Inc.	**US**	119,040	**538.5**
56	108.7	**43260**	ROUTERGATE Router Gate	**TR**	9,984	**477.7**
63	105.2	**10316**	CODERO-AS - Codero	**US**	31,232	**473.8**
611	50.0	**11565**	ASN-ALOT - ALOT, INC.	**US**	1,536	**448.7**

Мы рассматриваем категорию «Эксплоит-серверов» как наиболее важную среди анализа вредоносного кода, фишинга или любой другой злонамеренной активности в целом. Для исследования этой категории использовались дополнительные коэффициенты. Полностью с нашей методикой вы можете ознакомиться в Приложении 2.

Многие хосты и корпоративные серверы распространяют вредоносное ПО или осуществляют другие вредоносные действия из-за того, что были взломаны или скомпрометированы. Любая конфиденциальная информация, идентификационные и иные данные отправляются обратно на эксплоит-серверы и попадают в руки злоумышленников.

В отличие от спам-хостов эксплоит-серверы до недавнего времени были полностью расположены в странах с низким уровнем законодательной базы в области преследования киберпреступности. Однако, в отчете за второй квартал 2011 года 60% из Топ 10 крупнейших в этой сфере расположены в США.



9.1.4. Zeus-ботнеты

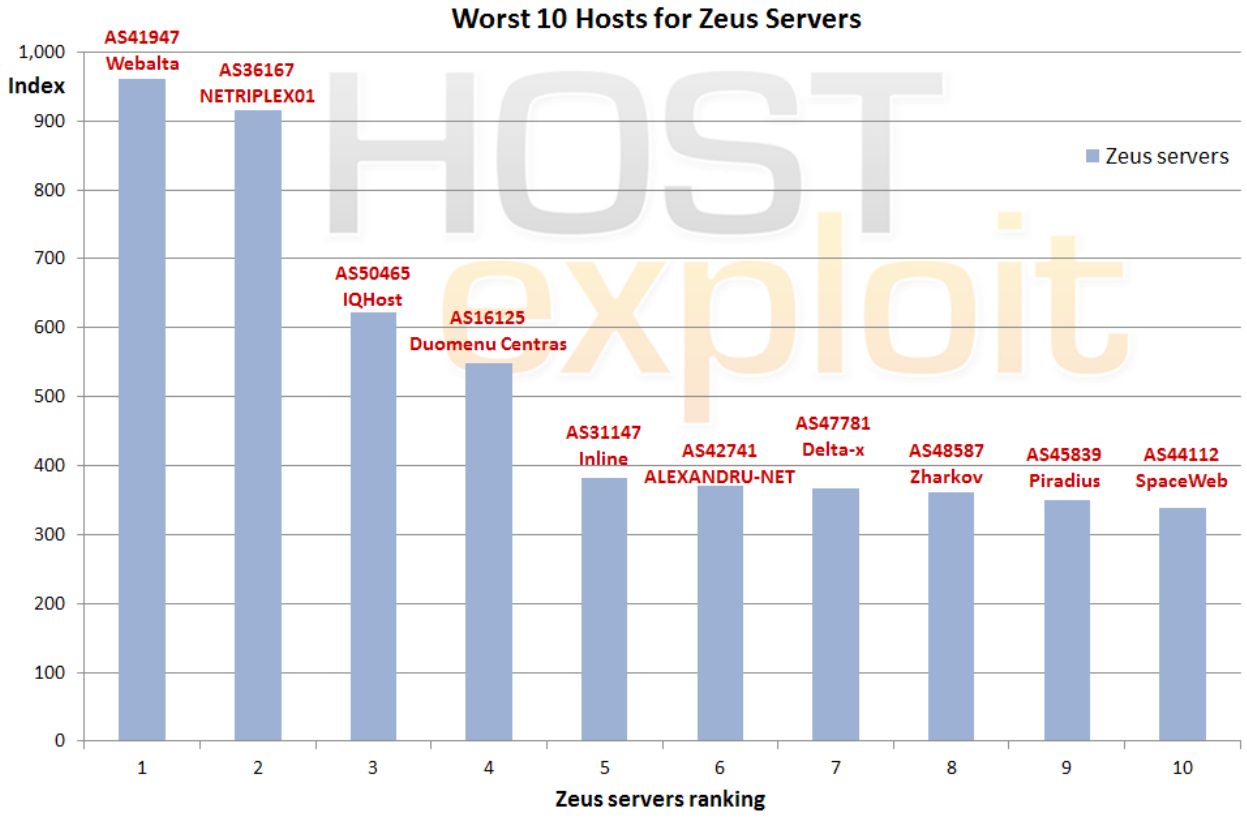
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
4	185.3	**41947**	WEBALTA-AS OAO Webalta	**RU**	16,128	**961.1**
8	170.9	**36167**	NETRIPLEX01 - NETRIPLEX LLC	**US**	46,080	**915.7**
109	85.2	**50465**	IQHOST IQHost Ltd	**RU**	1,024	**622.3**
159	76.9	**16125**	DC-AS UAB Duomenu Centras	**LT**	4,608	**549.4**
36	125.0	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	9,728	**381.9**
444	56.4	**42741**	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	**RO**	256	**370.7**
59	106.5	**47781**	ANSUA-AS DELTA-X Ltd	**UA**	512	**367.5**
95	90.0	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	**UA**	1,024	**361.2**
98	88.1	**45839**	PIRADIUS-AS PIRADIUS NET AS45839	**MY**	13,824	**349.8**
86	93.6	**44112**	SWEB-AS SpaceWeb JSC	**RU**	3,072	**339.0**

Киберпреступники управляют сетями зараженных компьютеров, называемыми «зомби», через серверы управления ботнетами. С одного сервера можно управлять примерно 250 000 или более подчиненными машинами. Мы выделили в данном отчете Zeus-ботнет, так как он по-прежнему остается наиболее дешевым и популярным на черном рынке.

Этот раздел следует рассматривать совместно с разделом 8.5 о эксплоит-серверах.

Не удивительно, если многие специалисты и исследователи найдут хорошо им знакомые серверы, перечисленные в списке Топ 10.

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



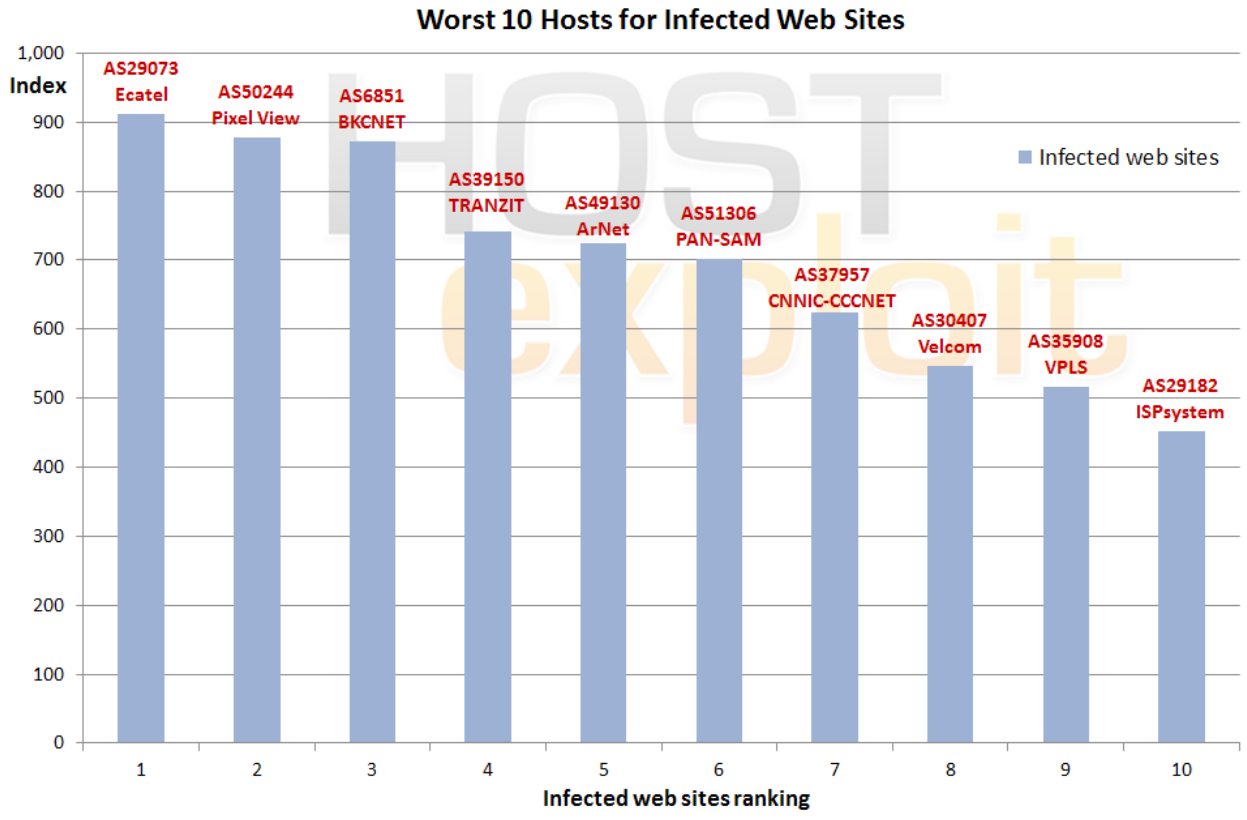
9.2.1. Зараженные сайты

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**911.6**
62	105.5	**50244**	ITELECOM Pixel View SRL	**RO**	7,936	**877.2**
16	161.1	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**871.4**
33	127.2	**39150**	TRANSIT-TELECOM-AS Tranzit Telecom LTD	**RU**	5,376	**741.2**
112	84.6	**49130**	ARNET-AS SC ArNet Connection SRL	**RO**	768	**724.2**
49	110.3	**51306**	UAIP-AS PAN-SAM Ltd.	**UA**	2,048	**701.4**
84	95.1	**37957**	CNNIC-CCCNET China Communication Co., Ltd	**CN**	4,096	**623.6**
82	96.7	**30407**	VELCOM - Rcp.net	**CA**	8,192	**546.7**
39	121.1	**35908**	VPLSNET - VPLS Inc. d	**US**	714,240	**515.6**
41	117.2	**29182**	ISPSYSTEM-AS ISPsystem Autonomous System	**RU**	35,840	**451.4**

Зараженные сайты — это обширная категория, в которой происходит вредоносная активность как через сознательное распространение вредоносного контента, так и через скомпрометированные сервисы, которые ничего об этом не подозревают.

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.

В таблице представлены как большие хосты, так и некоторое количество более мелких серверов, подозреваемых в преступной деятельности.

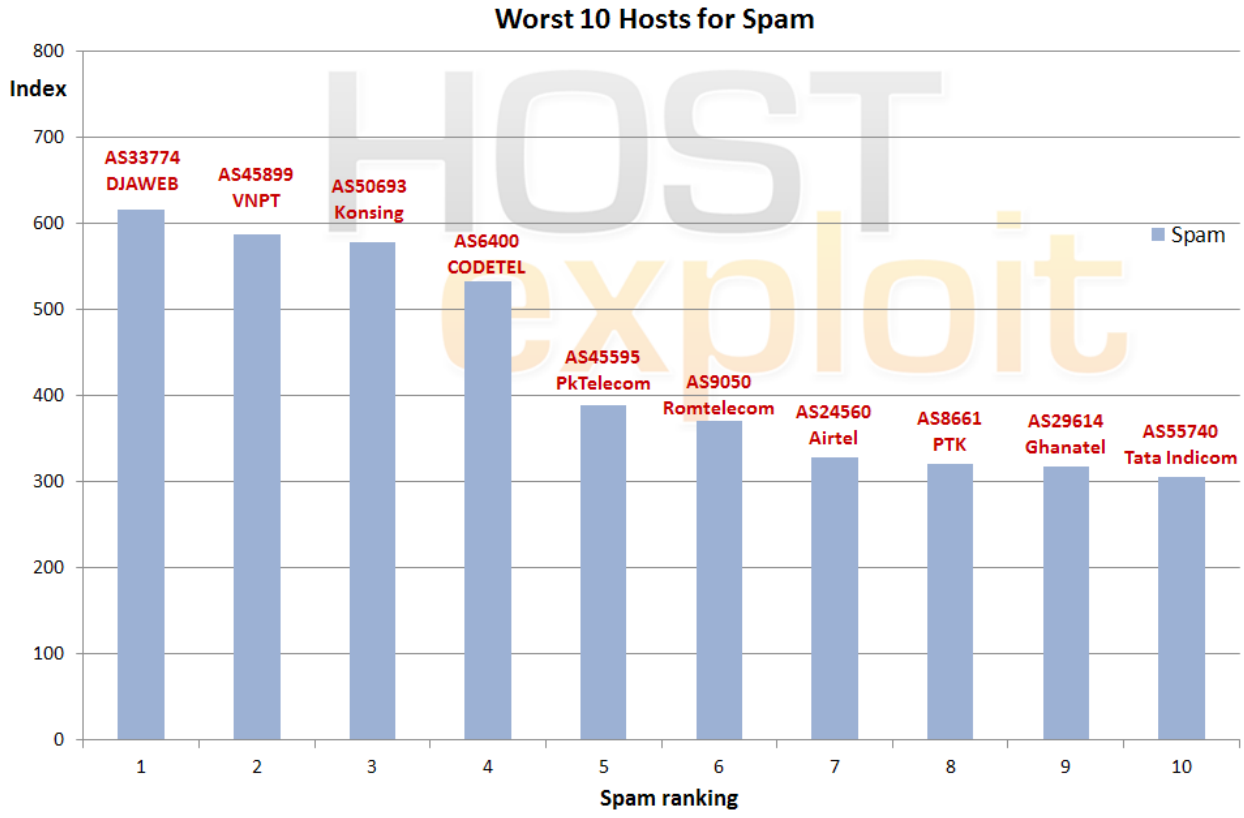


9.2.2. Спам

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
17	157.8	**33774**	DJAWEB	**DZ**	67,840	**616.1**
13	164.1	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,024,704	**587.7**
24	133.8	**50693**	KONSING-GROUP Konsing group doo	**SP**	2,048	**578.8**
34	126.2	**6400**	CompaÃ±Ãa Dominicana de TelÃ©fonos, C. por A. - CODETEL	**DO**	390,912	**533.0**
68	102.4	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	2,321,408	**388.3**
37	124.2	**9050**	RTD ROMTELECOM S.A	**RO**	1,645,824	**371.3**
45	114.4	**24560**	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	**IN**	1,810,432	**329.0**
176	74.2	**8661**	PTK PTK IP	**SP**	57,344	**321.4**
181	73.3	**29614**	GHANATEL-AS	**GH**	100,608	**317.5**
209	70.6	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	**IN**	246,784	**305.7**

Топ 10 показывает серверы, наиболее используемые спамерами. В странах, где данный вид деятельности законодательно не регулируется и не преследуется, спамеры используют проверенные и испытанные методы для предотвращения обнаружения их активности — fast-flux и одноразовые серверы. Кроме того, они быстро приспосабливаются к новым средствам распространения информации без необходимости применения каких-либо технических инноваций. Это отличает спамеров от иных компьютерных злоумышленников.

Один спам-сервер может причинить вреда больше, чем целая группа подобных серверов. Также при целевом использовании спам-рассылок даже небольшое количество спама может быть более эффективным, чем обыкновенная массовая рассылка. Эти две причины существенно усложняют количественное измерение спама. Поэтому мы объединяем наши результаты с результатами известных авторитетных источников — SpamHaus, UCEPROTECT-Network, Malicious Networks (FiRE) и SudoSecure. Результатом является полный текущий список мировых спам-серверов, то есть серверов, с IP-адресов которых происходит отправка спама.

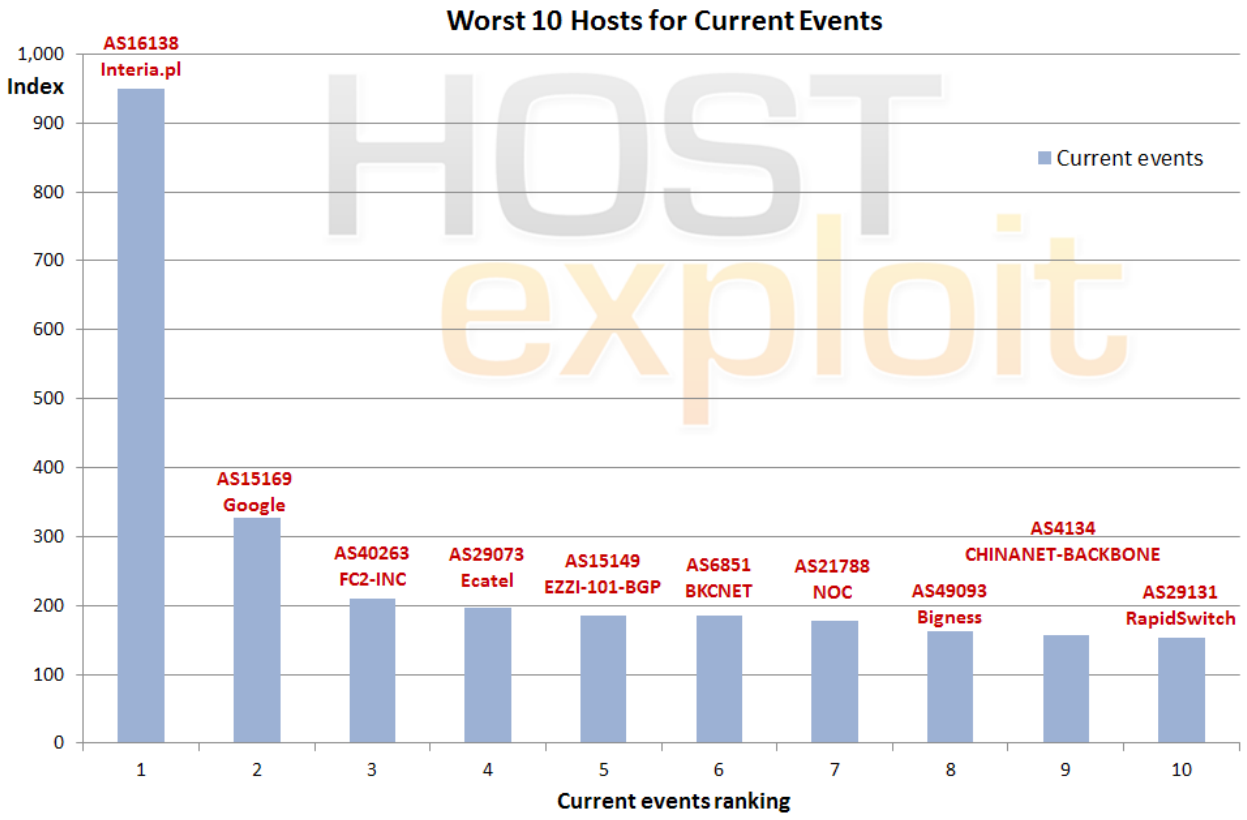


9.2.3. Текущие события

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
12	165.3	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**949.5**
35	125.6	**15169**	GOOGLE - Google Inc.	**US**	284,160	**328.1**
496	54.2	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.7**
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.1**
233	67.8	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**186.1**
16	161.1	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.3**
5	185.2	**21788**	NOC - Network Operations Center Inc.	**US**	282,624	**178.4**
320	60.6	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	512	**163.5**
21	155.3	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,796,608	**157.7**
65	104.7	**29131**	RAPIDSWITCH-AS RapidSwitch	**UK**	0	**152.3**

Категория текущих событий формируется из самых современных и быстро меняющихся угроз: 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.

Некоторые из перечисленных угроз присутствуют в хостах, упомянутых в таблице, которая содержит некоторые хорошо знакомые названия. Также стоит отметить, что 40% из этого Топ 10 расположены в США, а 20% — в Латвии, которая стала площадкой для хостинга серверов киберпреступников.



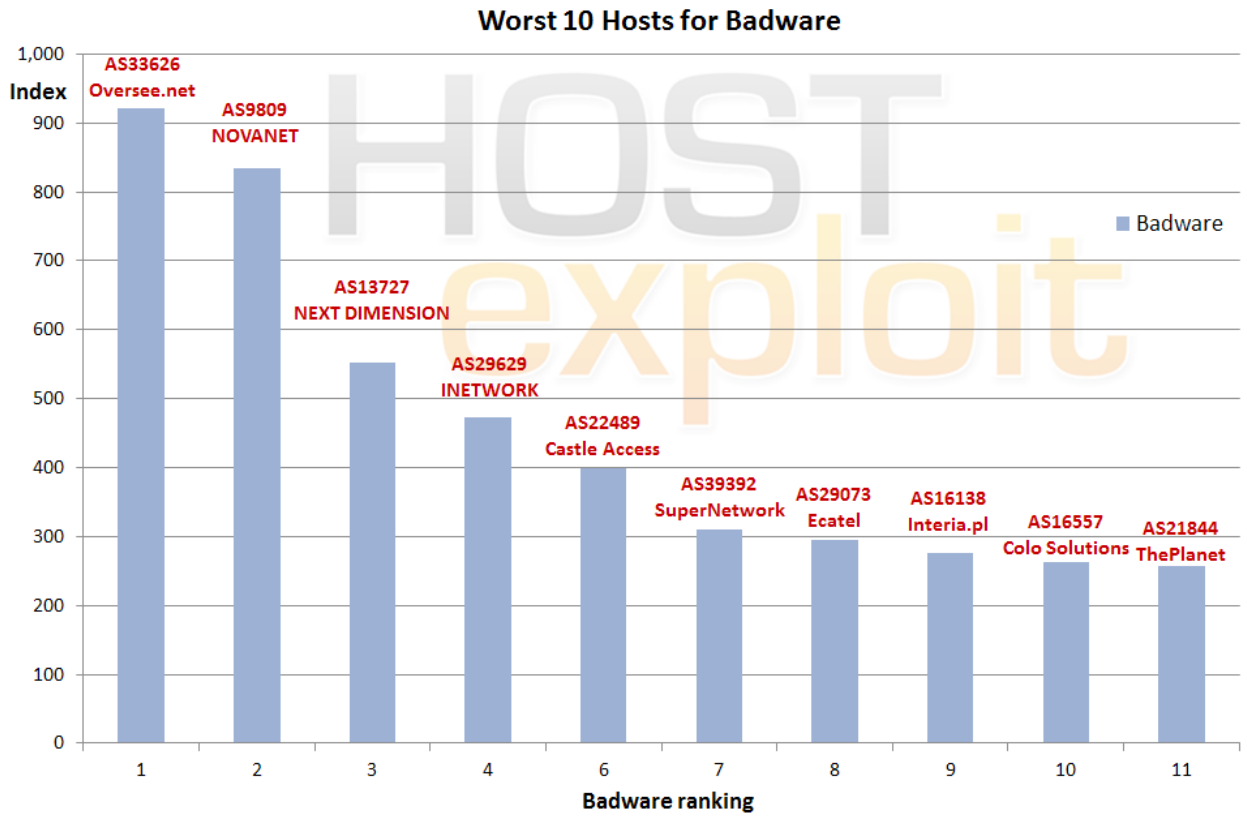
9.2.4. Вредоносное ПО

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
7	174.2	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**921.4**
10	168.3	**9809**	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	**CN**	11,008	**833.4**
23	145.8	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**553.2**
75	98.7	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**472.0**
26	132.5	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	48,384	**399.1**
79	97.8	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	49,920	**310.6**
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**294.2**
12	165.3	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**275.8**
118	82.8	**16557**	COLOSOLUTIONS - Colo Solutions, Inc.	**DE**	27,392	**263.2**
14	163.9	**21844**	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	**US**	1,548,800	**256.8**

Вредоносному ПО безразлично, каким образом пользователи могут использовать свой компьютер. Примерами такого программного обеспечения являются шпионские, вредоносные программы, программы-вымогатели и поддельная реклама. В большинстве случаев оно проявляется в виде бесплатных заставки, которые тайно генерируют рекламу, перенаправляют на нежелательные ресурсы, и программ слежки за вводом пользователя, которые передают введенные данные злоумышленникам.

В этом квартале продолжают наблюдаться «ложные срабатывания», особенно в отношении припаркованных доменов. Они были найдены в ограниченном количестве по сравнению с данными партнеров, и результаты начинают отражать это несоответствие.

Таблица в данной категории в первую очередь основана на данных от StopBadware, которые суммируют результаты от Google, Sunbelt Software и Team Cymru.



Серверы киберпреступников

10.1. Что такое серверы киберпреступников?

Серверы киберпреступников — это выделенные специализированные серверы или их часть, которые являются платформой для осуществления различного рода компьютерных преступлений. Серверы киберпреступников не являются зараженным хостом вследствие нарушения политики безопасности, а представляют собой целенаправленный инструмент осуществления преступной деятельности. При этом они иногда сами выступают в качестве хостинг-провайдеров и регистраторов.

Большое количество подобных примеров приведено в предыдущих отчетах HostExploit — Atrivo (US), McColo (US), Real Host (LV).

Интересно, что автономные системы, вошедшие в данный отчет, значительно меньше, чем представленные выше. Число IP-адресов данных АС находиться в диапазоне от 256 до 1024. Важно подчеркнуть, что большинство хостов из списка Топ 50 представляют собой организации, осуществляющих легальную деятельность.

10.2. Преступные сервера или зараженные хосты?

Исследования, содержащиеся в данном отчете, направлены на выявление зараженных хостов по всему миру. При составлении рейтинга Топ 50, предполагалось, что большинство хостинг-серверов являются легальными поставщиками услуг.

По сути, разница между понятиями «преступный сервер» и «зараженный хост» более ярко выражена в мотивах их владельцев. Владельцы первых могут быть идентифицированы как активно занимающиеся преступной деятельностью, в то время как зараженные хосты могут обвиняться только в недостатках политики безопасности, отсутствии или недостаточности мер по мониторингу сети или игнорировании жалоб со стороны пользователей.

10.3. Недействующие преступные серверы (все активны на конец первого квартала 2011; неактивны на конец второго квартала 2011)

AS number	Name
49469	SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup
43215	MONYSON GRUP SA
25402	CYBERNET ROMAINA
48709	XISOFT SRL
51699	ANTARKTIDA-PLUS LLC
51362	BESTISP PE Yastremskiy Leonid Stepanovich

10.4. Действующие преступные серверы

все активны на конец второго квартала 2011

AS number	Name	IPs	HE Rank
16138	INTERIAPL INTERIA.PL SA	4096	12
13727	ND-CA-ASN - NEXT DIMENSION INC	1024	23
50693	KONSING-GROUP Konsing group doo	2048	24
47781	ANSUA-AS DELTA-X Ltd	512	59
39150	TRANSIT-TELECOM-AS Tranzit Telecom LTD	5376	68
42741	ALEXANDRU-NET-TM-AS	256	84
48445	FAVN Favorit Network SL	256	92
48587	NET-0X2A-AS Zharkov Mukola Mukolayovuch	1024	95
50465	IQHOST IQHost Ltd	1024	109
49130	ARNET-AS SC ArNet Connection SRL	768	112
49093	BIGNESS GROUP LTD	512	295

Выводы

Второй квартал 2011 года характеризуется ростом взломов и атак типа отказ в обслуживании, осуществленными хакерскими группами, такими как Anonymous и LulzSec, а также менее известными преступными группировками. Но не все так плохо. Количество зараженных сайтов, по сравнению с аналогичным периодом прошлого года, снизилось. Это можно объяснить улучшением решений, позволяющих веб-мастерам обнаруживать подобные инциденты.

С точки зрения обнаруженных уровней опасности имеются некоторые изменения, если сравнить показатели первого и второго кварталов 2011г.

Главное изменение – это позиция №1 в списке самых зараженных хостов. Теперь это AS33182 HostDime, глобальный хостинг-провайдер, базирующий в США. HostDime возглавил список вследствие зафиксированной масштабной вредоносной активности, исходящей с его серверов. По факту, была обнаружена высокая активность в следующих категориях: спам, эксплоит-серверы, фишинговые серверы и ZEUS-серверы. При этом более низкая активность была замечена в следующих категориях: серверы управления ботнетами, вредоносное ПО и зараженные сайты.

В этом квартале HostDime лидирует по количеству хостов, осуществляющих преступную деятельность за пределами Соединенных Штатов Америки и поддерживаемых инфраструктурами легальных организаций. США является родиной для значительной части хостов из списка Топ 50. Эта цифра составляет почти половину (23) от общей суммы. Киберпреступники тянутся к хостинг-провайдерам тех стран, где относительно легко разместить веб-сайт, а также к тем, которые могут повысить уровень доверия к их сайтам.

Категория «Текущие события» измеряет количество хостов, вовлеченных в участие в самом современном и быстро меняющемся секторе вредоносной активности, такой как накрутка кликов, черный фарм-бизнес, новые сборники эксплоитов, SpyEye, ботнеты и смешанные атаки, такие как MALfi. Возглавляет эту категорию автономная система AS16138 Interia.pl.

Хосты и корпоративные сети не всегда сознательно занимаются вредоносной деятельностью, но могут распространять вредоносные программы с помощью взломанных или скомпрометированных серверов, составляющих часть «зомби»-сетей. Такие сети используются для дальнейшего распространения опасных или вредоносных воздействий, маскируя свое истинное происхождение и, таким образом, помогая избежать обнаружения. Эта категория, по мнению HostExploit самая важная с точки зрения анализа вредоносного ПО, фишинга и других опасностей. Возглавляет эту категорию в этом квартале AS14585 CIFNet, размещенная в Соединенных Штатах.

Тем не менее, некоторые известные системы показали значительное улучшение в плане снижения уровня зараженности. Наиболее отличилась AS47764 Netbridge, размещающая популярный почтовый сервис Mail.ru, который показал снижение Индекса на 84 процента. Наименьший уровень вредоносной активности в этом квартале показала AS34744 GVM Sistem, расположенная в Румынии.

Целью настоящего доклада является поднятие вопросов, что и почему позволяет злоумышленнику успешно осуществлять свою деятельность в сети Интернет. HostExploit и другие авторы, которые помогли в создании данного отчета, не считают закрытие «плохих» хостингов и интернет-провайдеров единственным решением растущей проблемы киберпреступности. Однако, публикация сравнительного и количественного списка хостов и интернет-провайдеров с точки зрения зараженности (подход «кто» и «где») помогает в понимании киберпреступности:

- Демонстрация сравнительных уровней зараженности, обнаруженных на интернет-хостах у интернет-провайдеров и в сетях, показывает, какая часть хостов участвует в преступной деятельности.
- Данный отчет и введенный Индекс НЕ выступают в качестве потребительского барометра для каждой из 38 030 автономных систем.
- Отчет предоставляет количественный анализ худших хостингов и сетей, которые не смогли предотвратить деятельность киберпреступников.
- Выпуск отчета о 50 худших хостов способствовал установлению обратной связи с некоторыми хостами и снижению их уровня опасности на 90%.
- Как было показано в предыдущих отчетах и немного затронуто в настоящем, количество выделенных преступных серверов и абузоустойчивых хостинговых компаний совсем невелико.

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

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.	Malware URL	Вредоносные URL	Высокая
3.	Abuse.ch	Сервера ZeuS	Высокая

4.	StopBadware	Образцы вредоносного ПО	Очень высокая
5.	SudoSecure	Спам-боты	Средняя
6.	Malicious Networks	Командные и управляющие сервера	Высокая
7.	Malicious Networks	Сервера фишинга	Средняя
8.	Malicious Networks	Сервера с эксплойтами	Средняя
9.	Malicious Networks	Сервера для рассылки спама	Низкая
10.	«HostExploit»	Текущие события	Высокая
11.	hpHosts	Образца вредоносного ПО	Высокая

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:

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

где:

B: *соотношение Байеса*

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

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

N: *количество зарегистрированных случаев*

N_a : *среднее количество зарегистрированных случаев в пробном наборе*

C: *вес IP-адреса = 20,000*

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

5 Вычисления

Для каждого источника информации рассчитываются 3 показателя.

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

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

где:

B_m : *максимальное соотношение Байеса*

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

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

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

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

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

где:

N_m : *максимальное количесвто станций в пробном наборе*

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

Индекс для каждого источника данных может быть рассчитан следующим образом:

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

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

Общий НЕ-индекс далее рассчитывается как:

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

где:

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