ECYFED

ISBN: 978-0-9836249-2-9

HostExploit Всемирный обзор киберпреступлений

Топ 50 «Самые плохие сети и хосты»

II квартал 2012

Отчет

"Data" - Graffiti Courtesy of cuatropiedos

GROUP IB

HOST exploit

CSIS

Содержание

HOST exploit

Топ 50

Обзор киберпреступлений

«Самые плохие сети и хосты»

CyberDefcon

Supported by

nominet trust

www.nominettrust.org.uk

Редактор

- Jart Armin

Рецензенты

- Dr. Bob Bruen
- Raoul Chiesa
- Peter Kruse
- Andre' DiMino
- Thorsten Kraft
- Ilya Sachkov

Использованные источники

- AA419
- Abuse.CH
- CIDR
- Clean-MX.DE
- Cyscon SIRT
- Emerging Threats
- Google Safe Browsing
- Group-IB
- HostExploit
- hpHosts
- ISC
- KnujOn
- MalwareDomains
- MalwareDomainList
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- SRI International
- StopBadware
- SudoSecure
- Team Cymru
- UCE Protect

Авторы

- Steve Burn
- Greg Feezel
- Andrew Fields
- David Glosser
- Niels Groeneveld
- Matthias Simonis
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson
- Michel Eppink
- DeepEnd Research

ECYFED

European Cyber Security Federation

ECYFED — международная федерация по противодействию киберугрозам и расследованию компьютерных преступлений. Объединяет CyberDefcon, Group-IB и CSIS.

О компании CyberDefcon

CyberDefcon является независимой организацией, чья миссия состоит в обеспечении безопасности в Интернете. Особое внимание уделяется устранению источников вредоносной активности. CyberDefcon предлагает широкий спектр специализированных услуг и решений для хостинг- и сервис-провайдеров с учетом индивидуальных потребностей клиентов.

О компании Group-IB

Основанная в 2003 году международная компания Group-IB — лидер российского рынка в области расследования компьютерных преступлений — оказывает полный комплекс услуг по расследованию компьютерных преступлений, начиная от оперативного реагирования на инцидент и заканчивая постинцидентным консалтингом. В составе компании работает Лаборатория компьютерной криминалистики и исследования вредоносного кода, оказывающая услуги независимой компьютерной экспертизы, в том числе и правоохранительным органам России. На базе Group-IB осуществляет свою деятельность CERT-GIB, круглосуточный центр быстрого реагирования на инциденты информационной безопасности. Входит в LETA Group.

О компании CSIS

Команда CSIS работает в соответствии с четырьмя базовыми принципами: ответственность, взаимное уважение, проактивный подход и позитивное отношение.

Этот корпоративный дух обеспечивает развитие бизнеса как внутри компании, так и во внешних взаимодействиях, одновременно помогая работать с клиентами и ежедневными новыми задачами, связанными с ИТ-безопасностью. Эти принципы являются базовыми ценностями и помогают создать надежную структуру для принятия базовых решений и разработки стратегий. Такой подход позволяет сформировать фундамент для всего бизнеса.

CSIS начала работать в Дании в 2003 году, и сегодня в компании трудится около 40 человек, находящихся на территории от Копенгагена до Сканнерборга. Каждый сотрудник CSIS играет важную и необходимую роль. Вместе мы создаем ту энергетику, которая позволяет нам привлекать и сохранять лучших профессионалов в области ИТ-безопасности.

ПРЕДУПРЕЖДЕНИЕ

Мы приложили все разумные усилия для обеспечения того, чтобы исходные данные, используемые в этом отчете, являлись актуальными, точными, полными и исчерпывающими на момент анализа. Тем не менее, в отчёте не подразумевается отсутствие ошибок, и используемые данные могут быть изменены без уведомления.

HostExploit не несет ответственности за данные, которые были искажены, неправильно истолкованы или изменены каким-либо образом. Сделанные выводы и основанный на этих данных анализ не следует рассматривать как приписываемые HostExploit или нашим партнёрам.

Введение

Сторонникам концепции международного взаимодействия в области информационной безопасности есть чему радоваться в этом квартале — в нескольких странах были успешно проведены операции против групп компьютерных злоумышленников, которые совершали свои преступления в течение длительного периода времени. Эти мероприятия являются нечто большим, чем просто элементом сотрудничества.

Слишком долго компьютерные преступники прикрывались тем, что государственные законы ограничены определенной территорией. Однако, в отсутствии каких-либо реальных изменений международного законодательства, по крайней мере, в ближайшее время, добровольно созданные партнерства открывают возможность для поимки некоторых из наиболее опасных преступников виртуального мира. (Подробности об этих историях вы можете найти в разделе «Новости»).

Раньше можно было говорить, что компьютерные преступники смогут долго действовать безнаказанно, используя недостатки международных законов, однако последние тенденции, определенно, принесут им плохие новости и, конечно, хорошие новости для всех пользователей компьютеров.

Практика добровольного международного взаимодействия будет расширяться по мере того, как дальнейшие успехи докажут эффективность обмена информацией на базовом уровне.

Впрочем, сейчас самое время представить подобную инициативу. Мы рады сообщить об учреждении Европейской федерации компьютерной безопасности ECYFED (European Cyber Security Federation), в которую войдет наш партнер CyberDefcon, компании Group-IB и CSIS . Вместе мы сможем более эффективно работать и исполнять свою миссию по ликвидации компьютерных угроз, используя объединенные ресурсы. ECYFED сейчас находится на начальном этапе планирования своей деятельности. Чтобы быть в курсе наших последующих мероприятий и узнать больше подробностей, вы можете посетить новый сайт http://ecyfed.com/

Jart Armin

Глобальная карта безопасности

Сфера компетенции HostExploit продолжает развиваться, мы постепенно укрепляем репутацию поставщика надежных данных, которым можно верить. Если вы еще не видели нашу Глобальную Карту Безопасности, представленную в апреле, вы можете оценить ее прямо сейчас. Карта уже получила позитивные отзывы из различных источников, и мы планируем расширить ее возможности благодаря серии улучшений.

Хотите принять участие?

Если вы поддерживаете то, что, что мы делаем, почему бы вам не стать спонсором или партнером HostExploit? Мы постоянно стремимся улучшить результаты нашей работы, расширяя сферу анализа. Если вы считаете, что можете помочь, мы рады будем рассмотреть любые ваши предложения.

Новости

Объединение экспертов против киберпреступности

Тот факт, что несколько группировок и крупнейших компьютерных преступников, использовавших вредоносную программу Carberp, были задержаны полицией, является основным достижением всех участников процесса — не только ведущей расследования Group-IB, но также многих партнеров компании, участвовавших в каждой из операций.

Троянская программа Carberp хорошо известна благодаря своим возможностям работы против систем интернет-банкинга. Начиная с 2009 года, она используется для атак на финансовые системы, работающие в режиме онлайн. Криминальные группы, использующие эту программу, получали колоссальную прибыль, исчисляющуюся несколькими миллионами в неделю. Вопрос пресечения такой активности стал высокоприоритетной задачей не только для российских банковских систем, оказавшихся основной мишенью злоумышленников, но и для банков из нескольких других стран, также пострадавших от Carberp.

Арест первой группировки Carberp был произведен в марте силами МВД и ФСБ России. Банда из 8 человек была уличена в использовании комбинации Win32/Carberp и Win32/RDPdoor с целью получения доступа к персональным компьютерам и огромному количеству систем дистанционного банковского обслуживания. Эта высокоорганизованная группировка снимала офис под видом легальной компании и содержала дропов для обналичивания похищенных денег через банкоматы в Москве.

В начале июня последовали новые аресты, связанные с Carberp, которые стали возможными за счет международного взаимодействия аналитиков из Group-IB, ESET и других компаний. В этот раз удалось задержать печально известную группировку Hodprot, работающую с 2008 года и ответственную за кражу более чем $3,7 миллионов с электронных банковских счетов. Преступники были задержаны МВД России в рамках расследования хищений средств у клиентов Сбербанка.

Позднее в июне Group-IB сообщила о третьем аресте компьютерных мошенников, использовавших Carberp. Сотрудники Управления «К» МВД России совершили рейд в Москве, конфисковав компьютеры и другие улики, подтверждающие криминальную деятельность злоумышленников. Одна из крупнейших бот-сетей, работавшая более 3 лет, была ликвидирована. Злоумышленники использовали модифицированную версию Carberp.

Известные в сети как Germes и Arashi, разработчики вредоносного ПО, создали многомиллионную банковскую бот-сеть, получившую в хакерских кругах название Origami. Они впервые использовали вредоносную программу RDPdoor для прямой кражи средств у пользователей систем интернет-банкинга, а также первыми применили Carberp со специальными инструментами загрузки, позволяющими обходить антивирус. В дополнение к этому группировка успешно перешла от эксплойтов Blackhole к Nuclear Pack, значительно увеличив количество зараженных компьютеров — до 6 миллионов в мае 2012 года. Количество активных зараженных машин в бот-сети доходило до 70 000.

Несмотря на то, что данные аресты проходили в России, для проведения операций активно привлекались исследователи из других стран. Лишь немногие действия компьютерных преступников могут происходить в одной стране, ведь Интернет не имеет границ. В качестве хорошего доказательства этого тезиса можно рассмотреть операцию ФБР против международной кардинговой сети, когда 26 июня одиннадцать граждан США были арестованы вместе с аналогичными одиннадцатью задержаниями в Великобритании, Боснии, Болгарии, Норвегии и Германии. Для проведения этого действительно международного расследования также были привлечены эксперты из многих других стран.

Полиция Болгарии провела операцию против группировки хакеров, называющих себя Cyber Warrior Invasion. Эта группа несет ответственность за более чем 500 атак на веб-сайты по всему миру, включая порталы крупнейших финансовых компаний. Расследование велось несколько месяцев. Группа использовала прокси-серверы, чтобы скрыть свое реальное местоположение и осуществить кражу конфиденциальной информации и данных о кредитных картах. Рейды были проведены в нескольких регионах Болгарии, все оборудование конфисковано. На одной из компьютерных систем, попавших в руки полиции, хранилась база данных почтовых адресов и аккаунтов в социальных сетях с паролями доступа. Она использовалась для шантажа и вымогательства.

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 зараженность, а не пропорциональную?

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

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

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

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

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

Почему данные хосты позволяют осуществлять зловредную деятельность?

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

Обратная связь приветствуется!

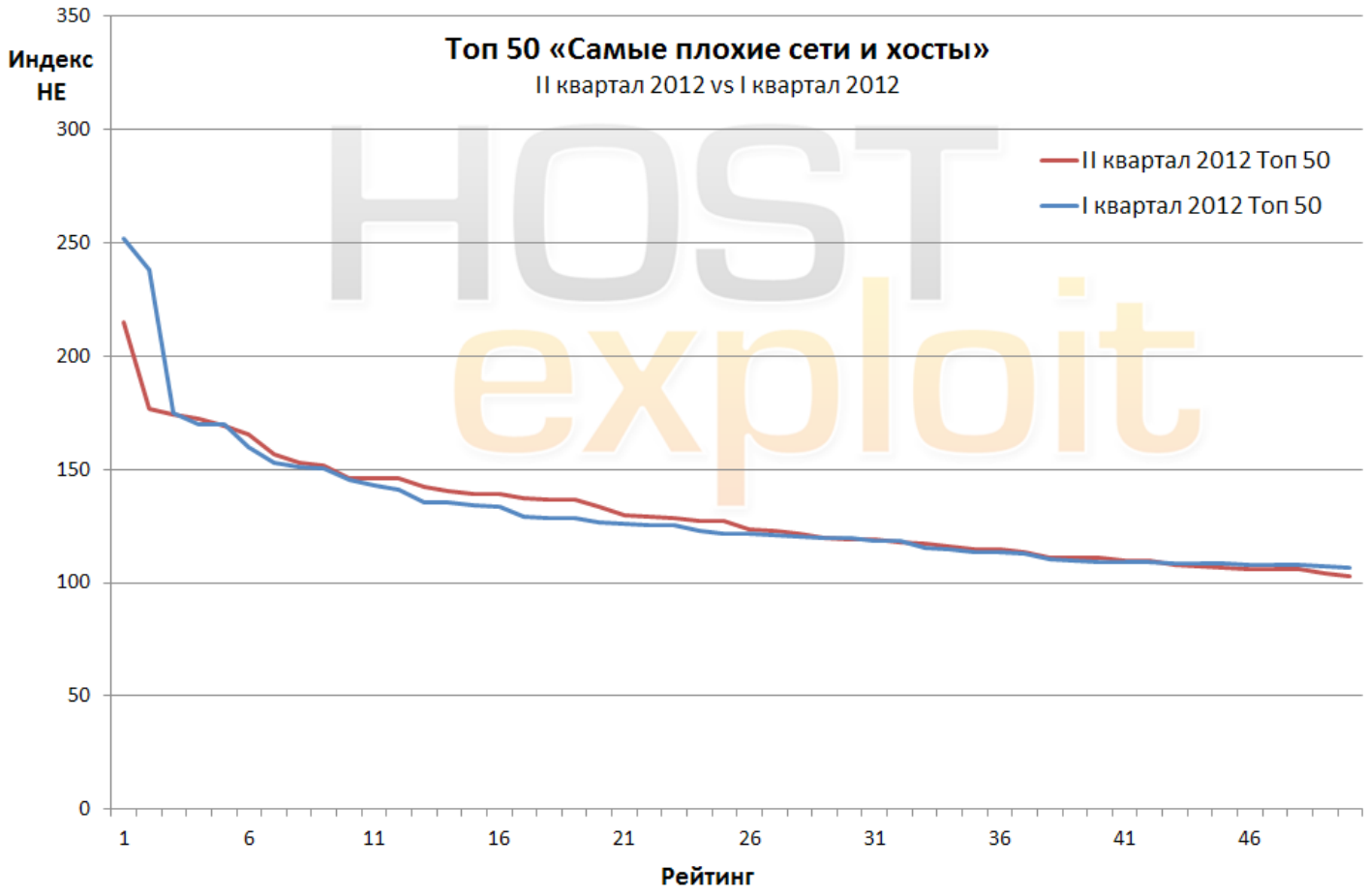
contact@hostexploit.com

info@group-ib.ru

4. Топ 50

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
▲ 1	214.67	41947	WEBALTA-AS OAO Webalta	RU	14,624
▲ 2	176.84	44112	SWEB-AS SpaceWeb JSC	RU	3,072
▲ 3	174.31	45538	ODS-AS-VN Online data services	VN	9,472
▲ 4	172.17	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,312
▼ 5	168.94	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▲ 6	165.34	39743	VOXILITY-AS Voxility SRL	RO	21,760
▲ 7	156.84	28753	LEASEWEB-DE Leaseweb Germany GmbH	DE	119,040
▲ 8	152.81	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	50,432
▲ 9	151.70	9891	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	TH	19,456
▲ 10	146.33	50465	IQHOST IQHost Ltd	RU	2,816
▼ 11	146.24	16125	DC-AS UAB Duomenu Centras	LT	5,376
▼ 12	145.81	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	50,432
▲ 13	142.53	48031	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	UA	17,664
▲ 14	140.29	43146	AGAVA3 Agava Ltd.	RU	18,176
▲ 15	139.24	43362	MAJORDOMO MAJORDOMO LLC	RU	2,560
▼ 16	138.95	32475	SINGLEHOP-INC - SingleHop	US	295,168
▲ 17	137.25	47781	ANSUA-AS DELTA-X Ltd	UA	1,536
▲ 18	136.49	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▼ 19	136.35	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,218,048
▲ 20	133.78	48159	TIC-AS Telecommunication Infrastructure Company	IR	2,048
▲ 21	129.49	35415	WEBAZILLA WebaZilla European Network	CY	63,488
▼ 22	128.95	24940	HETZNER-AS Hetzner Online AG RZ	DE	570,368
▲ 23	128.76	16265	LEASEWEB LeaseWeb B.V.	NL	331,776
▼ 24	127.45	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,539,328
▲ 25	127.07	44368	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	SE	3,072
▶ 26	123.43	34201	PADICOM PADICOM SOLUTIONS SRL	RO	6,400
▲ 27	123.00	15169	GOOGLE - Google Inc.	US	562,688
▲ 28	121.30	38731	VTDC-AS-VN Vietel - CHT Compamy Ltd	VN	33,024
▲ 29	119.99	21788	NOC - Network Operations Center Inc.	US	297,216
▲ 30	119.10	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,408
▲ 31	118.79	6939	HURRICANE - Hurricane Electric, Inc.	US	736,512
▲ 32	118.15	48716	PS-AS PS Internet Company Ltd.	RU	512
▲ 33	117.18	29671	SERVAGE Servage GmbH	DE	12,288
▲ 34	115.85	40676	PSYCHZ - Psychz Networks	US	26,624
▼ 35	114.74	9809	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	CN	10,752
▲ 36	114.57	49335	NCONNECT-AS Navitel Rusconnect Ltd	RU	12,288
▼ 37	113.72	16276	OVH OVH Systems	FR	937,216
▲ 38	111.04	12695	DINET-AS Digital Network JSC	RU	298,624
▼ 39	111.00	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	113,033,184
▲ 40	110.84	57169	EDIS-AS-EU EDIS GmbH	AT	7,936
▼ 41	109.83	32613	IWEB-AS - iWeb Technologies Inc.	CA	235,520
▲ 42	109.72	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	CN	53,795,584
▼ 43	107.54	32181	ASN-GIGENET - GigeNET	US	42,240
▲ 44	107.24	44553	SNS-BG-AS Smart Network Solutions Ltd.	BG	3,840
▲ 45	106.71	29182	ISPSYSTEM-AS ISPsystem Autonomous System	LU	39,168
▲ 46	105.97	35569	PETERHOST-MOSCOW Concorde Ltd.	RU	2,048
▲ 47	105.75	26105	Telecarrier, Inc	PA	44,608
▼ 48	105.70	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	IN	262,144
▼ 49	103.89	22489	CASTLE-ACCESS - Castle Access Inc	US	47,872
▼ 50	103.06	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840

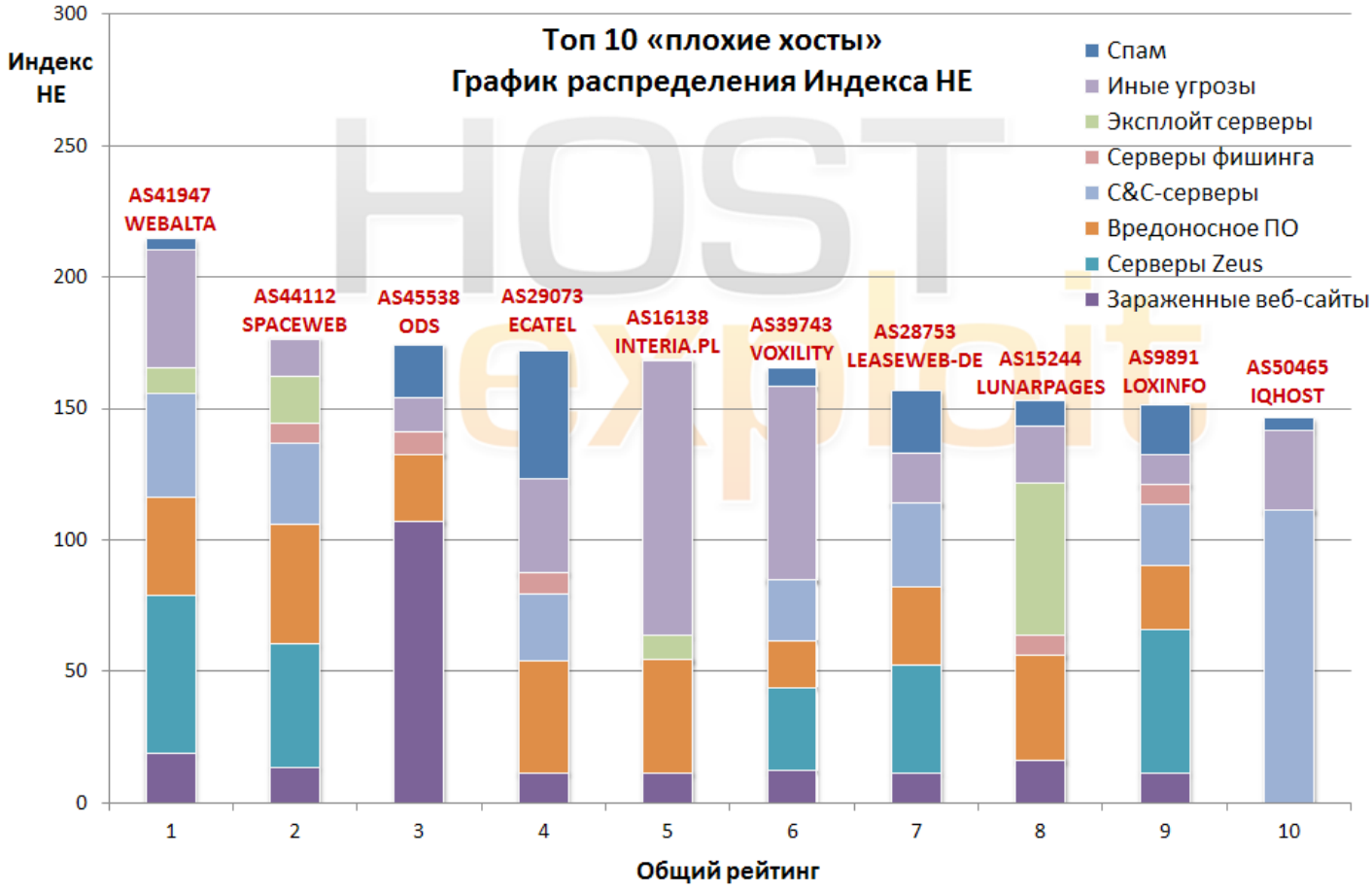
Сравнение Q2 2012 и Q1 2012



Сравнение отчетов Топ 50 «Самые плохие хосты», выпущенные в июне и марте 2012 года.

Несмотря на ряд значимых перемещений хостов в Топ 50, общая картина распределения вредоносной активности осталась практически без изменений.

График распределения Индекса HE



Таблица, приведенная выше, отражает распределение позиций в первой десятке согласно Индексу HE.

Она показывает эффективность применения взвешенных значений для различных категорий, что обеспечивает сбалансированность Индекса HE. Это можно увидеть, обратив внимание на отсутствие основных источников «вредоносности» для большинства хостов.

Данный график наглядно показывает, почему каждый из хостов в Топ 10 имеет столь высокий рейтинг.

Например, вы можете видеть, что AS41947 WEBALTA, которая заняла место #4 в I квартале 2012 года, теперь поднялась на позицию #1 в связи с высокой концентрацией вредоносного ПО и иных угроз (включая XSS и RFI).

Еще одним примером служит AS45538 ODS (Vietnam), которая теперь занимает место #3 (а в I квартале 2012 была на позиции #186) в основном за счет огромной концентрации зараженных веб-сайтов.

Что нового?

7.1. Обзор

	Предыдущий квартал - Q1 2012			Текущий квартал - Q2 2012		
	Номер	**Название**	**Страна АС**	**Номер**	**Название**	**Страна АС**
#1	**16138**	Interia.pl	**PL**	**41947**	Webalta	**RU**
#2	**47583**	Hosting Media	**LT**	**44112**	SWEB	**RU**
#3	**33182**	HostDime	**US**	**45538**	ODS	**VN**
#1 Спам	**31133**	MegaFon	**RU**	**41859**	TIC	**IR**
#1 C&C-серверы	**47583**	Hosting Media	**LT**	**50465**	IQHost	**RU**
#1 Серверы Zeus	**16125**	Duomenu Centras	**LT**	**34201**	Padicom	**RO**
#1 Серверы фишинга	**9280**	Connect Infobahn Australia	**AU**	**43362**	Majordomo	**RU**
#1 Эксплойт серверы	**3.537**	Infium	**UA**	**2607**	Slovak Academic Network	**EU**
#1 Вредоносное ПО	**9809**	Nova Network	**CN**	**9809**	Nova Network	**CN**
#1 Зараженные веб-сайты	**16138**	Interia.pl	**PL**	**45538**	Online data services	**VN**
#1 Иные угрозы	**16138**	Interia.pl	**PL**	**16138**	Interia.pl	**PL**

Исследование поквартальных тенденций дает нам возможность определить, насколько ответственно провайдеры относятся к предоставлению хостинга.

Для администрации ответственного хоста будет шоком узнать, что они были оценены невероятно высоко или даже хуже – заняли место #1. Этого может быть достаточно для немедленной реакции и исправления.

Нам хотелось бы думать, что ответственность провайдеров является причиной смены лидеров в различных категориях. Однако, к сожалению, многие хосты, бывшие на первых местах, смогли переместиться лишь на несколько позиций вниз, позволив новым именам получить сомнительное преимущество находиться в начале списка. Новые лидеры, безусловно, заслужили этого, продемонстрировав действительно высоки уровни концентрации угроз. Тем временем AS9809 Novanet и AS16138 Interia твердо заняли первые места в категориях «Вредоносное ПО» и «Иные угрозы» соответственно.

7.2. Вновь зарегистрированные хосты

К концу II квартала 2012 года было зарегистрировано **41 635** автономных систем, что на **957** больше по сравнению с концом I квартала 2012 года.

Ниже вы можете видеть перечень 10 систем, зарегистрированных во II квартале и обладающих наиболее высокими Индексами HE. В связи с высокой вредоносной активностью, отмеченной за небольшой отрезок времени, эти хосты вызывают большой интерес.

Приведенный ниже список 10 автономных систем повторяет результаты двух предыдущих квартальных отчетов.

Интересно также отметить, что в трех последних квартальных отчетах из 30 недавно зарегистрированных хостов шесть систем более не существует.

	Рейтинг HE	Индекс HE	Номер AC	Название AC	Страна AC	Количество IP
2012 Q2	107	84.5	57668	SANTREX-AS Santrex Internet Services Ltd.	GB	1,280
	1,090	38.2	39365	MICROLINES-AS MICROLINES ISP	LV	8,192
	1,201	35.6	57972	WEBEXXPURTS Deepak Mehta FIE	EE	10,752
	1,485	30.5	132241	SKSATECH1-MY SKSA TECHNOLOGY SDN BHD	MY	1,024
	1,731	26.4	34934	UKFAST UKFast.Net Ltd	GB	27,648
	1,789	25.7	33667	CMCS - Comcast Cable Communications, Inc.	US	0
	1,863	24.8	33659	CMCS - Comcast Cable Communications, Inc.	US	8,192
	2,057	23.0	54444	AVESTA-NETWORKS-LLC - Avesta Networks LLC	US	6,144
	2,338	20.6	132116	ANINETWORK-IN Ani Network Pvt Ltd	IN	1,024
	2,440	20.0	34170	AZTELEKOM Azerbaijan Telecomunication ISP	AZ	36,096
2012 Q1	274	67.0	48031	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	UA	16,640
	653	50.8	12327	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business international	GB	4,608
	906	44.6	49087	PODCEM-AS Open JSC "Podilskiy Tcement"	UA	256
	1,337	35.3	24768	ALMOUROLTEC ALMOUROLTEC SERVICOS DE INFORMATICA E...	PT	2,048
	1,828	27.8	51699	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	UA	256
	1,875	27.3	49236	RELNET-AS TOV "Leksim"	UA	256
	1,948	26.4	57704	SPEED-CLICK-LTD SpeedClick for Information Technology and...	IL	2,048
	2,053	25.4	31408	ORANGE-PALESTINE Orange Palestine Group Co. for Technological...	PS	1,024
	2,212	24.0	37385	SONITEL	NE	8,960
	2,260	23.7	34109	AS34109 CB3ROB Ltd. & Co. KG	NL	9,216
2011 Q4	740	46.7	21508	COMCAST-21508 - Comcast Cable Communications Holdings, Inc	US	256
	1,356	34.0	4213	VPLSNET-EAST - VPLS Inc. d	US	2,048
	1,644	29.2	27626	AS-JOYTEL - Joytel	US	1,024
	1,986	25.2	57374	GIV-AS Commercial radio-broadcasting company Cable operator...	MK	7,168
	2,063	24.4	47311	ASBRESTRW Transport Republican unitary enterprise...	BY	256
	2,181	23.6	4.459	--No Registry Entry--	BR	256
	2,189	23.5	43463	BST-AS Biuro sprendimu tinklas UAB	LT	3,072
	2,406	21.9	57446	TELEMONT-AS Telemont Service S.R.L.	EU	4,096
	2,596	20.6	28015	MERCO COMUNICACIONES	AR	22,528
	2,905	18.7	3.961	ENERGOMONTAZH-AS ENERGOMONTAZH ltd.	EU	256

7.3. Улучшившиеся хосты

Изменение	Предыдущий квартал		Текущий квартал		Номер AC	Название AC	Страна AC	Количество IP
	Позиция	Индекс	Позиция	Индекс				
-78.4%	2	238.2	600	51.4	47583	HOSTING-MEDIA Aurimas Rapalis "II Hosting...	LT	4,096
-75.1%	107	86.0	2,239	21.4	197145	ASINFIUM Infium Ltd.	UA	9,728
-74.5%	72	94.1	1,933	24.0	13174	MTSNET OJSC "Mobile TeleSystems" Auton...	RU	26,368
-72.9%	127	80.0	2,208	21.7	25159	SONICDUO-AS AS for MegaFon-Moscow	RU	10,240
-66.7%	135	78.5	1,757	26.1	48587	NET-0X2A-AS Private Entrepreneur Zharkov...	UA	1,024
-64.5%	48	107.8	1,091	38.2	27990	Hosting Panama	PA	5,632
-63.2%	90	88.7	1,354	32.6	24203	NAPXLNET-AS-ID PT Excelcomindo Pratama...	ID	22,528
-63.2%	115	82.8	1,484	30.5	27956	Cyber Cast International, S.A.	PA	3,840
-61.5%	60	100.1	1,080	38.5	31163	MF-KAVKAZ-AS JSC MegaFon	RU	5,632
-60.7%	87	89.9	1,213	35.4	13301	UNITEDCOLO-AS UNITED COLO GmbH	DE	66,816

Хосты, указанные в таблице выше, все без исключения показали значительное сокращение уровня вредоносной активности за три месяца, прошедшие с момента публикации нашего отчета за I квартал 2012 года.

Многие виды вредоносной активности могут быть неразрывно связанными друг с другом, в результате чего некоторые хосты просто не могут самостоятельно их обнаружить. Однако мы поддерживает старания этих 10 наиболее улучшивших свои показатели хостов, которые существенно отличаются размерами, местом положения, видом бизнеса и категориями вредоносного контента, с которыми им удалось справиться. Они показали, что, несмотря на все сложности, можно сократить уровень вредоносной активности, приложив дополнительные усилия и освободившись от шаблонного мышления.

Примечательны следующие улучшения:

- AS47583 HOSTING-MEDIA Aurimas Rapalis "II Hosting Media" (Литва) опустилась с позиции #2 на #600. Это прекрасное улучшение, особенно в свете того, что данный хост входил перечень 50 самых плохих хостов по результатам многих предыдущих отчетов.
- AS197145 ASINFIUM Infium Ltd. (Украина) показала значительное снижение Индекса НЕ на 75,1%, что позволило данному хосту перейти на позицию #2239 с позиции #107. Это стало возможным благодаря ликвидации эксплойт-серверов для уязвимости Black Hole, а также другим усилиям компании. Однако данный хост по-прежнему размещает серверы управления бот-сети ICE9.

7.4. Ухудшившиеся хосты

Изменение	Предыдущий квартал		Текущий квартал		Номер AC	Название AC	Страна AC	Количество IP
	Позиция	Индекс	Позиция	Индекс				
12888.0%	30,182	1.0	20	133.8	48159	Telecommunication Infrastructure Company	IR	2,048
12044.3%	35,872	0.9	44	107.2	44553	SNS-BG-AS Smart Network Solutions Ltd.	BG	3,840
1342.1%	5,445	8.2	32	118.2	48716	PS-AS PS Internet Company Ltd.	RU	512
429.4%	2,216	24.0	25	127.1	44368	ASDELTAMANAGEMENT DELTA MANAGEMENT	SE	3,072
275.6%	2,343	23.3	92	87.4	11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc	US	28,416
244.5%	1,459	33.3	36	114.6	49335	NCONNECT-AS Navitel Rusconnect Ltd	RU	12,288
238.6%	2,167	24.4	116	82.7	34941	CYBERCOM-AS CyberCom & YT AB	SE	2,048
209.7%	2,054	25.4	135	78.8	50939	SPACE-AS Space Ro Srl	RO	1,792
207.4%	1,792	28.3	95	87.1	47894	VERITEKNIK VeriTeknik Bilisim Ltd.	TR	4,096
201.7%	2,086	25.2	153	76.0	47781	ANSUA-AS DELTA-X Ltd	UA	1,536

Перечисленные здесь хосты показали наихудшую динамику и увеличение уровня вредоносной активности по сравнению с предыдущим кварталом. Мы рекомендуем этим хостам пересмотреть свои недавние изменения, чтобы выяснить причину внезапного роста вредоносной активности. Недавно зарегистрированные хосты рассмотрены в разделе 7.2.

Самым «выдающимся» хостом этого квартала стал AS48159 Telecommunication Infrastructure Company (Иран), скакнувший с позиции #30182 (из 41635 возможных) на #20. Это стало возможным за счет выхода на место #1 по рассылке спама во всем мире.

AS44553 SNS-BG-AS Smart Network Solutions Ltd показал буквально невероятный рост в связи со значительным увеличением количества размещаемых серверов C&C, а также рассылкой спама

Топ 10 стран

Наша новейшая методология позволяет более точно выявить уровни вредоносной активности, присутствующей в автономных системах конкретной страны. Этот параметр связан с определенными сложностями, такими как невозможность точного определения физического местоположения сервера в автоматическом режиме.

Однако, с определенными оговорками, можно получить достаточно ценные результаты.

Ранее мы выявляли «худшие» страны, просто суммируя количество хостов, попавших в перечни Топ 50 и Топ 250 и принадлежащих к определенному региону. Очевидно, такой подход значительно ухудшал результаты тех стран, в которых больше хостов. А это противоречит духу нашего отчета, целью которого является освещение концентрации вредоносной активности.

Итак, что же мы изменили в этот раз? Теперь мы рассматриваем каждую страну также как и отдельные системы, учитывая общее количество IP-адресов и вредоносных элементов во всех системах, принадлежащих к этой стране. После этого мы вычисляем индекс каждой страны, используя такую же методологию, как и для отдельных систем.

В качестве результата мы получаем "Индекс страны", отражающий уровень вредоносной активности в промилле, не слишком привязываясь к количеству хостов, размещенных в данной стране.

Ниже приведена таблица, содержащая Топ 10 «худших» стран согласно данной методологии расчета: она является лишь небольшим фрагментом результатов, содержащихся на сайте Global Security Map, где можно найти полный перечень стран и их индексов.

Данные о стране			Оценка	
Страна АС	**Название**	**Количество IP**	**Позиция**	**Индекс**
RU	**RUSSIAN FEDERATION**	50,552,160	**1**	**359.3**
LU	**LUXEMBURG**	1,104,128	**2**	**315.6**
LV	**LATVIA**	1,770,752	**3**	**255.8**
UA	**UKRAINE**	14,088,192	**4**	**251.5**
VG	**VIRGIN ISLANDS, BRITISH**	11,264	**5**	**247.1**
TH	**THAILAND**	16,298,225	**6**	**233.9**
TR	**TURKEY**	20,522,752	**7**	**233.7**
RO	**ROMANIA**	12,217,344	**8**	**229.5**
MD	**MOLDOVA, REPUBLIC OF**	1,126,400	**9**	**225.5**
NL	**NETHERLANDS**	23,865,088	**10**	**209.7**

«Чистые» хосты

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP
36,966	**0.520**	**3300**	BT-INFONET-EUROPE BT-Infonet-Europe	**SE**	700,288
34,085	**0.592**	**38333**	SYMBIO-AS-AU-AP Symbio Networks	**AU**	139,360
31,424	**0.610**	**42362**	ALANIA-AS Sevosetinelectrosvyaz	**RU**	112,640
31,076	**0.618**	**10970**	LIGHTEDGE - LightEdge Solutions	**US**	103,680
31,073	**0.619**	**7821**	ZAYO-MN - Onvoy	**US**	102,912
30,463	**0.630**	**14390**	CORENET - Coretel America, Inc.	**US**	92,672
12,218	**0.664**	**262914**	Comision Federal de Electricidad	**MX**	68,864
12,176	**0.670**	**16360**	SATLYNX_GMBH Satlynx GmbH	**DE**	66,048
11,971	**0.671**	**18268**	JANIS Naganoken Kyodou Densan Co.Ltd.	**JP**	65,536
11,966	**0.688**	**8641**	NAUKANET-AS LLC Nauka-Svyaz	**RU**	57,600

9.1. Для чего нужна таблица «чистых» хостов?

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

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

Данные раздел является постоянной частью нашего отчета.

9.2. Критерии отбора

Мы отбираем «чистые» хосты среди интернет-провайдеров, хостинг провайдеров или организаций, которые владеют минимум 10000 выделенными IP-адресами. Многие хостинг-провайдеры, представленные в других разделах данного отчета, 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.

Плохие хосты по категориям

10.1.1. C&C-серверы

Рейтинг HE	Индекс HE	Номер AC	Название AC	Страна AC	Количество IP	Индекс
10	146.3	**50465**	IQHOST IQHost Ltd	**RU**	2,816	**1,000.0**
190	71.0	**50297**	CITONET Centr Informacionnyh Technologii, Ltd.	**UA**	5,120	**596.1**
250	66.6	**13209**	ATOM-HOSTING Atom Hosting SRL	**RO**	768	**491.7**
434	56.5	**56617**	ASVPSHOSTING SIA "VPS Hosting"	**LV**	1,024	**487.4**
44	107.2	**44553**	SNS-BG-AS Smart Network Solutions Ltd.	**BG**	3,840	**446.4**
160	75.1	**46785**	QUASAR-DATA-CENTER - QUASAR DATA CENTER, LTD.	**US**	4,608	**436.8**
323	61.6	**10103**	HKBN-AS-AP HK Broadband Network Ltd.	**HK**	19,712	**435.9**
11	146.2	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**427.8**
104	84.8	**26230**	TOTTAWA - Telecom Ottawa Limited	**CA**	22,272	**419.2**
153	76.0	**39388**	OTEL-AS Forcraft Ltd.	**BG**	8,704	**394.5**

Категория «Серверы управления бот-сетями» показывает распределение данного вида угроз в сетях различных провайдеров. Наши собственные данные, главным образом, объединены с информацией, предоставленной Shadowserver.

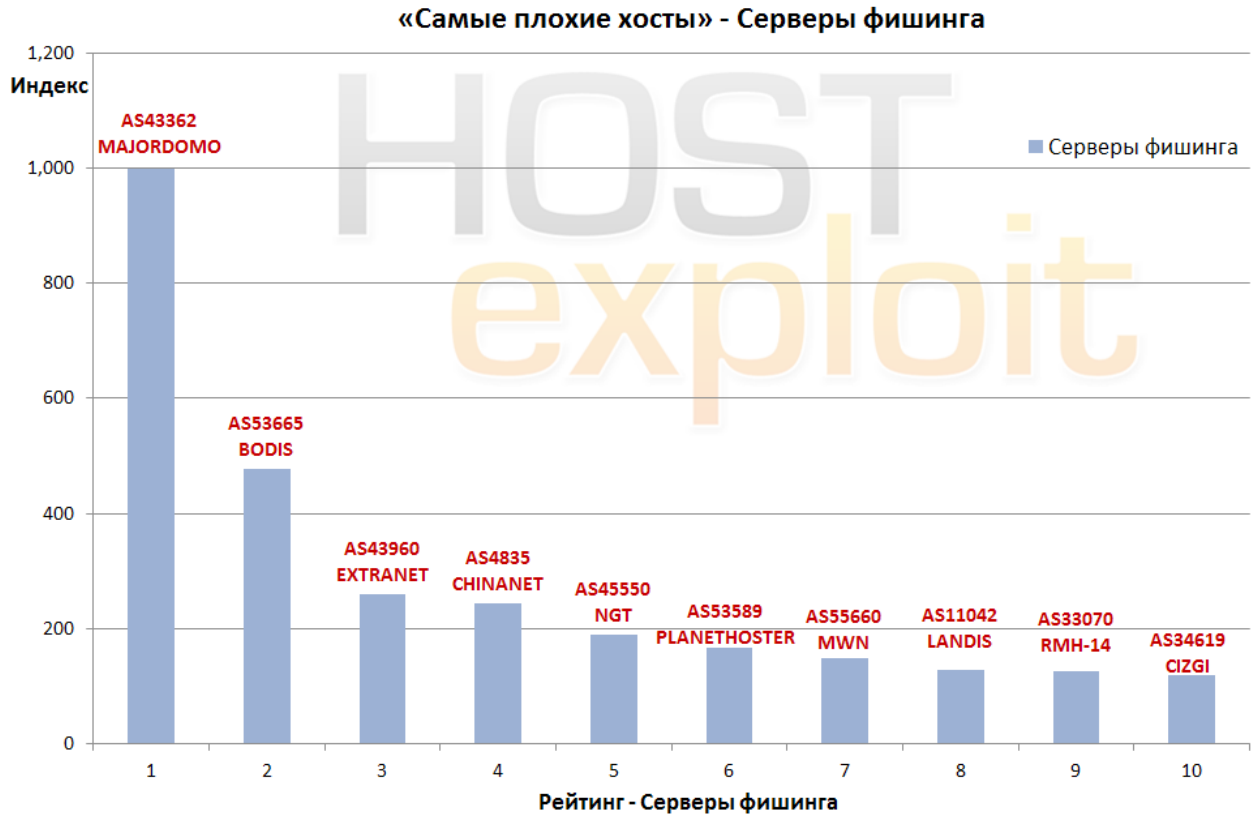
AS50465 IQHOST (Российская Федерация) возглавляет данную категорию в связи с исключительно большим количеством C&C-серверов в собственных сетях. AS44553 SNS Smart Networks Solutions Ltd перепрыгнул целый ряд позиций и занял место #4 в данной таблице и #43 в общем рейтинге. Этот хост впервые попал в Топ 50, хотя в I квартале был на позиции #35872.

10.1.2. Фишинг-серверы

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
15	139.2	**43362**	MAJORDOMO MAJORDOMO LLC	**RU**	2,560	**1,000.0**
309	62.6	**53665**	BODIS-1 - Bodis, LLC	**CN**	1,024	**477.3**
2,449	19.9	**43960**	EXTRANETCTC Consorzio Terrecablate	**IT**	2,048	**260.3**
314	62.3	**4835**	CHINANET-IDC-SN China Telecom (Group)	**CN**	103,456	**244.2**
1,453	30.8	**45550**	NGT-AS-VN New Generations Telecommunications Corporation	**VN**	1,280	**188.9**
737	47.6	**53589**	PLANETHOSTER-8 - PlanetHoster	**CA**	3,328	**165.8**
760	46.8	**55660**	MWN-AS-ID PT Master Web Network	**ID**	1,280	**148.6**
92	87.4	**11042**	LANDIS-HOLDINGS-INC - Landis Holdings Inc	**US**	28,416	**128.9**
138	78.6	**33070**	RMH-14 - Rackspace Hosting	**US**	512,768	**125.7**
73	93.3	**34619**	CIZGI Cizgi Telekomunikasyon Hizmetleri Sanayi Ve Ticaret...	**TR**	28,672	**118.0**

Фишинг и социальная инженерия продолжают создавать сложности для банков и корпораций всех размеров, так как киберпреступники применяют все новые и новые способы кражи информации, чтобы получить доступ к денежным средствам.

В этом квартале все хосты в Топ 10 по данной категории сменились на новые. Большой скачек вверх совершил хост AS43960 EXTRANETCTC (Италия) из-за большого количества фишинг-серверов. Также следует отметить присутствие AS53665 BODIS, который расположился на месте #2. Он зарегистрирован в Китае, но направляет трафик через США. Первую позицию занимает AS43362 MAJORDOMO (Россия), обнаруживший исключительно большое количество фишинг-серверов.



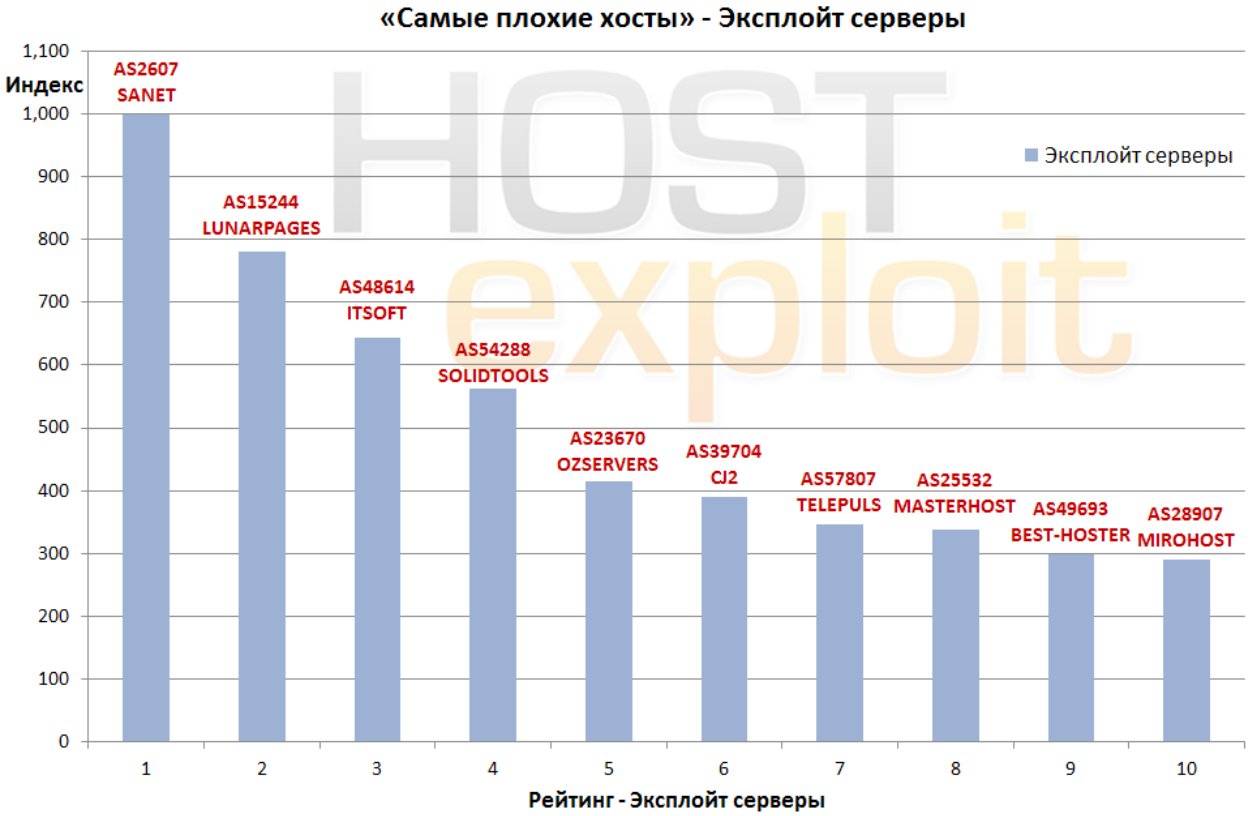
10.1.3. Эксплойт-серверы

Рейтинг HE	Индекс HE	Номер AC	Название AC	Страна AC	Количество IP	Индекс
54	102.6	**2607**	SANET Slovak Academic Network	**EU**	526,080	**1,000.0**
8	152.8	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	50,432	**780.4**
135	78.8	**48614**	ITSOFT-AS ITSoft Ltd.	**RU**	2,048	**643.9**
486	55.2	**54288**	SOLIDTOOLSINC - SolidTools Technology, Inc.	**US**	16,640	**562.7**
171	73.7	**23670**	OZSERVERS-AU Oz Servers, Data Centres, Australia Wide	**AU**	16,384	**415.7**
198	70.7	**39704**	CJ2-AS CJ2 Hosting&Development	**NL**	6,400	**389.5**
815	45.0	**57807**	TELEPULS-AS Telepuls "Spider" sp. z o.o. S.K.A.	**PL**	6,656	**345.8**
62	97.4	**25532**	MASTERHOST-AS .masterhost autonomous system	**RU**	77,824	**338.0**
122	81.7	**49693**	BEST-HOSTER Best-Hoster Group Co. Ltd	**RU**	2,048	**298.0**
151	76.4	**28907**	MIROHOST Internet Invest Ltd.	**UA**	11,776	**289.3**

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

Хосты и корпоративные серверы могут пересылать вредоносное ПО или выполнять другие злонамеренные действия в результате взлома или компрометации. Важная информация, учетные данные жертв и другие данные, полученные нелегальным способом, передаются на эксплойт-серверы с помощью вредоносного ПО.

Обратите внимание, что по сравнению с I кварталом в таблице появились новые хостинг-провайдеры. Серьезные изменения в этой категории могут быть результатом компрометации серверов. AS2607 SANET переместилась с позиции #940 в I квартале на #52 во II квартале за счет высокой концентрации эксплойт-серверов, что и стало причиной ее лидерства в данной категории.



10.1.4. Серверы Zeus

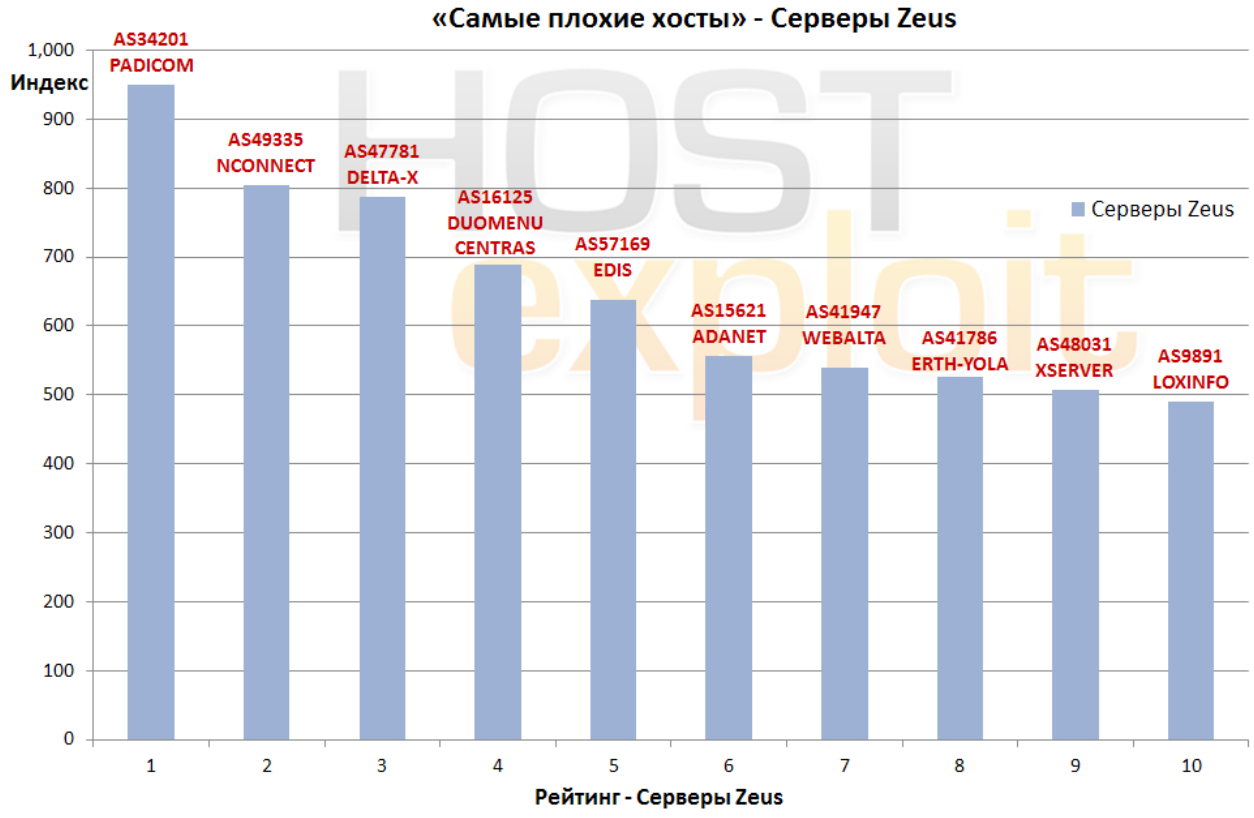
Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
26	123.4	**34201**	PADICOM PADICOM SOLUTIONS SRL	**RO**	6,400	**950.0**
36	114.6	**49335**	NCONNECT-AS Navitel Rusconnect Ltd	**RU**	12,288	**804.1**
17	137.2	**47781**	ANSUA-AS DELTA-X Ltd	**UA**	1,536	**787.2**
11	146.2	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**688.3**
40	110.8	**57169**	EDIS-AS-EU EDIS GmbH	**AT**	7,936	**637.4**
64	97.0	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	13,312	**556.1**
1	214.7	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**540.1**
141	78.3	**41786**	ERTH-YOLA-AS CJSC "ER-Telecom Holding"	**RU**	36,096	**526.5**
13	142.5	**48031**	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	**UA**	17,664	**507.2**
9	151.7	**9891**	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	**TH**	19,456	**490.3**

Киберпреступники управляют сетями зараженных компьютеров, известных также как «зомби», отделяя саму бот-сеть от серверов управления. Один C&C-сервер может управлять более чем 250 000 зараженных компьютеров. При этом бот-сеть Zeus остается самым дешевым и популярным решением на черном рынке.

Этот раздел необходимо рассматривать вместе с разделом 9.1.3, посвященным эксплойт-серверам.

Отличительной особенностью в данной категории является доминирование сервис-провайдеров, зарегистрированных в странах Восточной Европы. При этом некоторые уже известные здесь автономные системы несколько изменили свои позиции, чтобы освободить путь зарегистрированной в России AS49335 NCONNECT Navitel Rusconnect Ltd.

AS41947 Webalta продолжает держаться в десятке лидеров данной категории, размещая серверы Zeus и C&C.



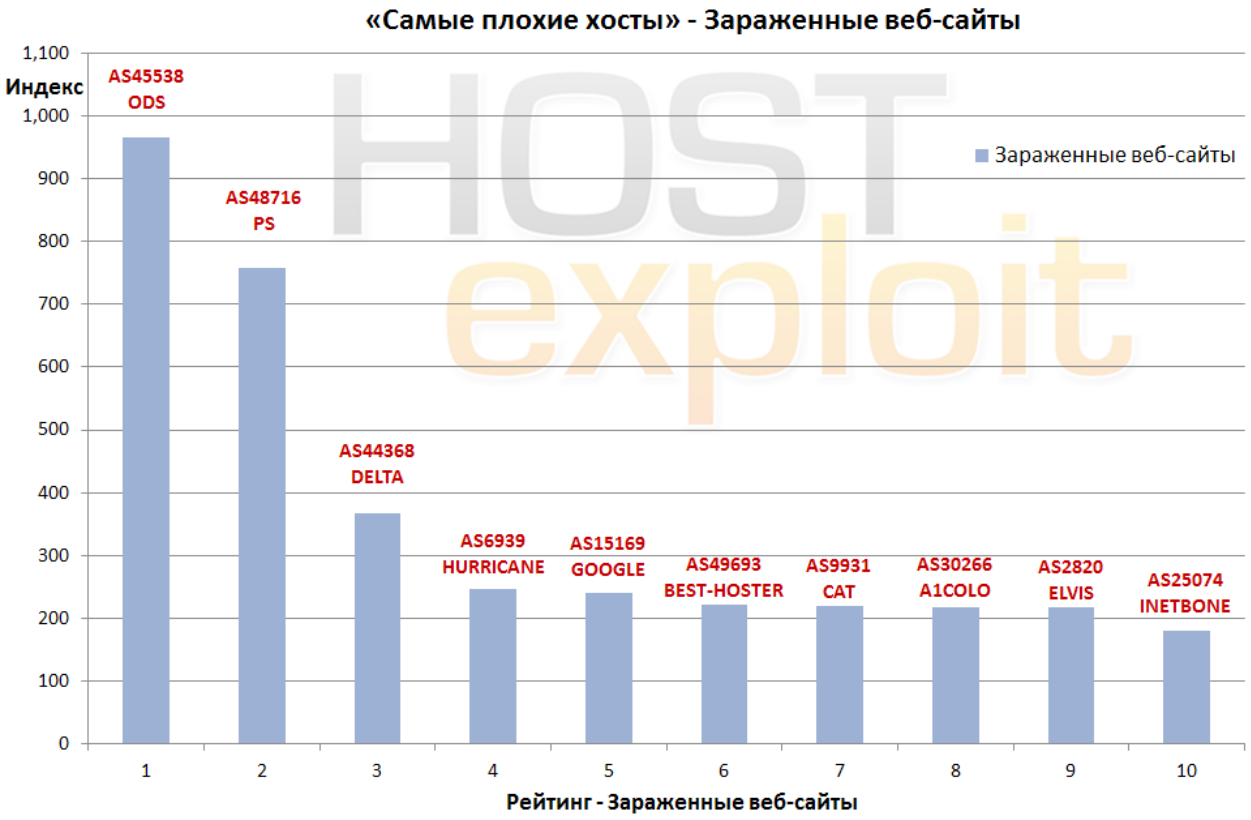
10.2.1. Зараженные веб-сайты

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
3	174.3	**45538**	ODS-AS-VN Online data services	**VN**	9,472	**965.8**
32	118.2	**48716**	PS-AS PS Internet Company Ltd.	**RU**	512	**758.6**
25	127.1	**44368**	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	**SE**	3,072	**368.0**
31	118.8	**6939**	HURRICANE - Hurricane Electric, Inc.	**US**	736,512	**247.4**
27	123.0	**15169**	GOOGLE - Google Inc.	**US**	562,688	**241.1**
122	81.7	**49693**	BEST-HOSTER Best-Hoster Group Co. Ltd	**RU**	2,048	**221.4**
30	119.1	**9931**	CAT-AP The Communication Authoity of Thailand, CAT	**TH**	209,408	**220.3**
303	63.0	**30266**	A1COLO-COM - A1COLO.COM	**US**	8,192	**217.8**
887	43.5	**2820**	ELVIS-AS ZAO "Elvis-Telecom"	**RU**	51,712	**216.4**
58	100.1	**25074**	INETBONE-AS MESH GmbH	**DE**	104,960	**179.1**

«Зараженные веб-сайты» представляют собой ту категорию, в которой могут присутствовать сразу несколько форм вредоносной активности. Это может происходить в рамках сознательного распространения вредоносного контента или в результате взлома и компрометации.

В этом разделе данные нашего собственного исследования, собранные из специальных ловушек, объединены с информацией, полученной от Clean-MX и hphosts.

В этом квартале не слишком известные имена присутствуют вместе с очень знакомыми. Позиция #1 в данной категории досталась AS45538 ODS Online Data Services, что объясняет, почему этот провайдер перепрыгнул на место #3 в общем рейтинге.



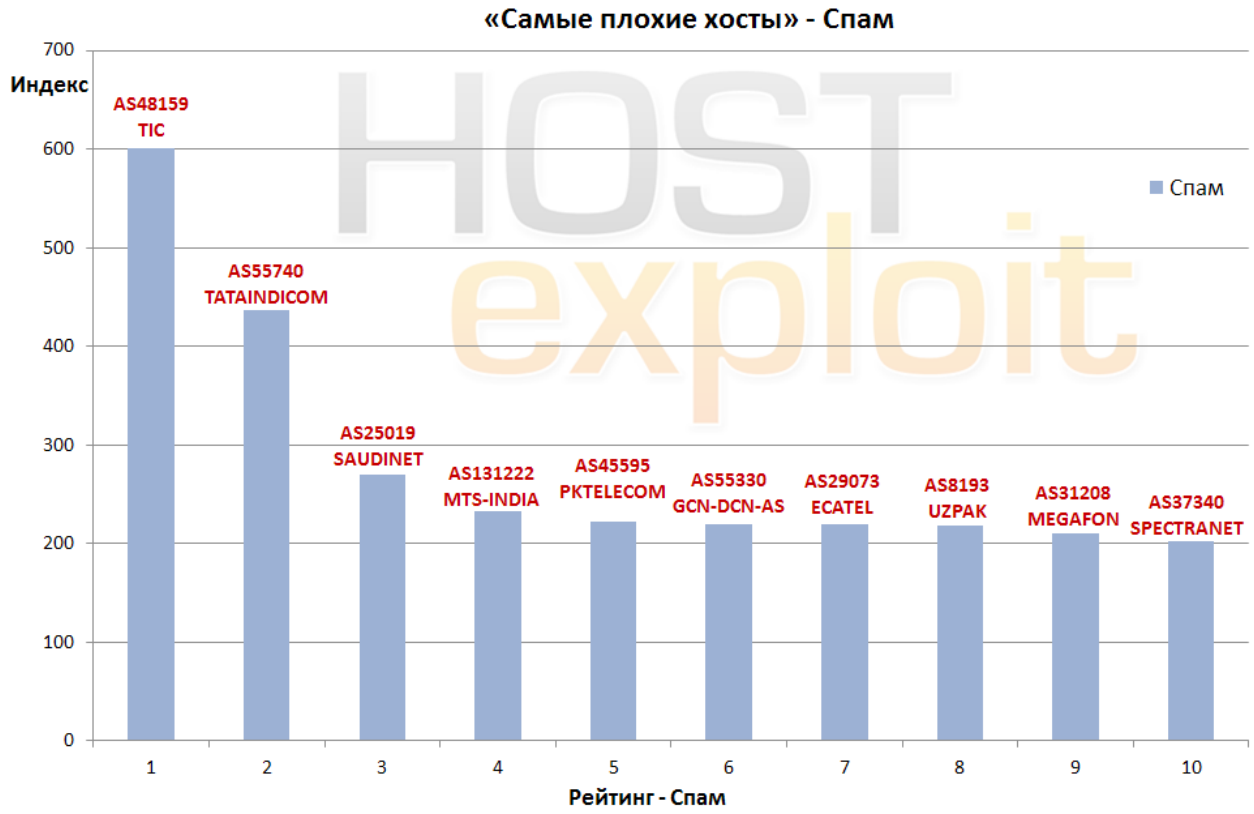
10.2.2. Спам

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
20	133.8	**48159**	TIC-AS Telecommunication Infrastructure Company	**IR**	2,048	**601.1**
48	105.7	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM	**IN**	262,144	**436.6**
119	82.2	**25019**	SAUDINETSTC-AS Autonomus System Number for SaudiNet	**SA**	5,357,056	**269.8**
591	51.6	**131222**	MTS-INDIA-IN 334,Udyog Vihar	**IN**	404,992	**232.3**
419	57.6	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,745,024	**222.1**
692	49.0	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT...	**AF**	19,200	**219.8**
4	172.2	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**219.8**
607	51.3	**8193**	UZPAK Uzpak Net	**UZ**	26,112	**217.5**
754	46.9	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	4,096	**210.0**
808	45.2	**37340**	Spectranet	**NG**	5,120	**202.7**

Спамеры стараются использовать серверы, расположенные в странах с минимальным регулированием и уровнем мониторинга, что позволяет им действовать, не боясь наказаний

И хотя этот паттерн сохранился в целом, во II квартале сложилась интересная ситуация. Место #1 в данной категории занял хост AS48159 TIC, зарегистрированный в Иране, в стране, известной четким мониторингом сетей. Значит ли это, что в системе защиты есть «слепое пятно», допускающее такую активность, или причина кроется в чем-то другом?

Также хочется отметить возвращение AS29073 Ecatel в список Топ 10 в данной категории.



10.2.3. Иные угрозы

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
5	168.9	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**940.1**
6	165.3	**39743**	VOXILITY-AS Voxility SRL	**RO**	21,760	**659.6**
51	102.8	**24282**	KIR Kagoya Japan CO,LTD	**JP**	23,808	**630.4**
648	50.3	**12327**	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business...	**EU**	4,608	**447.7**
514	54.2	**50244**	ITELECOM Pixel View SRL	**RO**	7,936	**424.8**
1	214.7	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**404.9**
526	53.6	**44571**	AKRINO-AS Akrino Inc	**VG**	1,024	**361.0**
699	48.8	**26499**	MOMENTOUS - MOMENTOUS	**CA**	10,752	**332.2**
180	72.4	**29568**	COMTEL-AS SYSNET SECURE S.R.L.	**RO**	17,664	**327.4**
4	172.2	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**322.3**

Самые современные и быстро меняющиеся виды и векторы атак формируют категорию «Иные угрозы».

Здесь HostsExploit учитывает такие злонамеренные действия как MALfi (XSS/RCE/RFI/LFI), XSS-атаки, скликивание, черный фарм-бизнес, поддельные антивирусы, Zeus (Zbota), Artro, SpyEye, Ice9, Stuxnet, DuQu, черный SEO, а также целый спектр новых наборов для взлома, представляющих собой ключевой компонент для данной категории.

Применение широкого спектра техник позволило выделить Топ 10 хостов, который содержит хорошо известные имена.

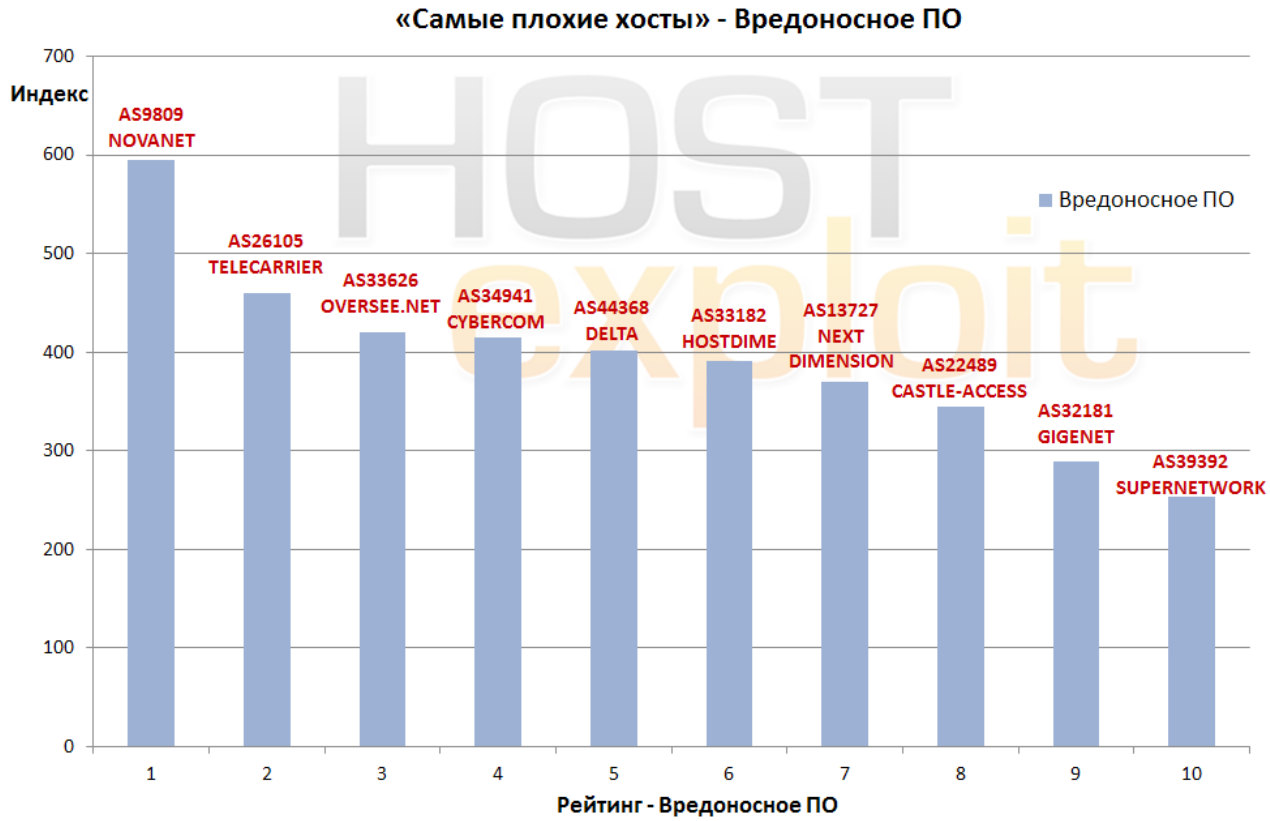
В предыдущих отчетах в данной категории лидировали хосты, размещенные в США. Но во II квартале 2012 года большинство систем из перечня Top 10 располагаются в Европе, а две системы — в Азии.

10.2.4. Вредоносное ПО

Рейтинг НЕ	Индекс НЕ	Номер АС	Название АС	Страна АС	Количество IP	Индекс
35	114.7	**9809**	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	**CN**	10,752	**594.7**
47	105.8	**26105**	Telecarrier, Inc	**PA**	44,608	**459.3**
50	103.1	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**419.5**
116	82.7	**34941**	CYBERCOM-AS CyberCom & YT AB	**SE**	2,048	**415.5**
25	127.1	**44368**	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	**SE**	3,072	**401.9**
12	145.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	50,432	**391.5**
128	80.5	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**370.0**
49	103.9	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	47,872	**344.4**
43	107.5	**32181**	ASN-GIGENET - GigeNET	**US**	42,240	**288.7**
127	80.5	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	53,504	**253.5**

Вредоносное ПО индифферентно к тому, как пользователь хочет использовать свой компьютер. Примерами такого ПО являются шпионские программы, вирусы, мошеннические программы и назойливая реклама. Обычно оно распространяется в виде бесплатных заставок для рабочего стола, которые начинают показывать рекламу, перенаправлять браузер на неожиданные страницы, а также загружать клавиатурных шпионов, чтобы передавать персональные данные злоумышленникам.

В этом квартале снова отличились те же правонарушители, включая AS9809 NOVANET (Китай), занявшая место #1 уже второй раз подряд, а также AS33626 OVERSEE, получившая позицию #3. Теперь к ним присоединились AS26105 TELECARRIER (Панама) на месте #2 и AS34941 CYBERCOM (Швеция) на #4.



Заключение

В этом квартале мы наблюдали одновременно и успешную работу, и провалы.

Всегда приятно видеть, что бывший хост #1 снижает объемы вредоносности и выходит из рейтинга Топ 50, как это произошло с AS47583 HOSTING-MEDIA. К несчастью, на позицию #1 всегда выходит кто-то новый, которая как раз и досталась AS41947 WEBALTA.

В I квартале 2011 года WEBALTA возглавляла список, однако хост добился хороших результатов, вычищая мусор из своих сетей, что позволило ему понизить свою позицию в рейтинге. Очень печально видеть, что после всего этого WEBALTA вернулась на место #1. Мы будем надеяться, что обнаружив себя на этой позиции, администрация данной системы предпримет новые действия против недавно появившихся проблем, благодаря которым выросло количество иных угроз и C&C-серверов.

Позитивной тенденцией можно считать улучшение позиций провайдеров, зарегистрированных в США. В этом квартале ни одну категорию не возглавил американский хост. Общее количество хостов из США в рейтинге Топ 50 снизилось с 17 в I квартале до 13 во втором. Очевидно, отдельные хосты из США, такие как AS15222 ADDD2NET (занимающий самое высокое место — #8), все еще требуют тщательной работы. Но, по крайней мере, мы можем говорить о хорошей тенденции.

Не столь хорошо показали себя хосты, зарегистрированные в России, заняв три места в рейтинге Топ 10, включая позиции #1 и #2. Несмотря на успех недавно завершившегося дела против группировки Carberp, в России необходимо провести еще много работы, чтобы очистить сетевые системы.

Напоследок нам хотелось бы отметить отключение серверов бот-сети Grum. Хотя это событие произошло не в рамках II квартала, оно достойно внимания. Постоянные рассылки спама были прекращены благодаря совместным действиям различных сообществ, что еще раз демонстрирует возможность успешного партнерства.

Jart Armin

Приложение 1

Словарь

Автономная система (Autonomous System)

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

Вредоносное программное обеспечение (Badware):

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

«Черные списки» (Blacklists):

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

Ботнет (Botnet):

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

Межсайтовая подделка запроса (CSRF):

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

Система доменных имен (DNS):

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

Черный список DNS (DNSBL):

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

Эксплойт (Exploit):

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

Хостинг (Hosting):

Услуга по предоставлению вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети (обычно Интернет). Обычно под

понятием услуги хостинга подразумевают как минимум услугу размещения файлов сайта на сервере, на котором запущено ПО, необходимое для обработки запросов к этим файлам (веб-сервер). Как правило, в услугу хостинга уже входит предоставление места для почтовой корреспонденции, баз данных, DNS, файлового хранилища и т. п., а также поддержка функционирования соответствующих сервисов.

IANA:

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

ICANN:

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

IP (Internet Protocol):

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

IPv4:

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

IPv6:

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

Интернет-провайдер (ISP):

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

LFI (Local File Inclusion):

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

MALfi (Malicious File Inclusion):

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

Вредоносные ссылки (Malicious Links):

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

MX:

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

NS (Name Server):

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

Open Source Security:

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

Фарм-бизнес (Pharming):

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

Фишинг (Phishing):

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

Регистрация доменных имен (Registry):

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

Регистратор доменных имен (Registrars):

Это компания с полномочиями регистрации доменных имен, уполномоченная ICANN.

Remote File Inclusion (RFI):

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

Мошенническое программное обеспечение (Rogue Software):

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

Rootkit:

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

Sandnet:

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

Спам (Spam):

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

Троян (Trojans):

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

Червь (Worms):

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

XSA (Cross Server Attack):

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

Приложение 2

1 Последовательность изменений

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

Таблица 1: Последовательность изменений

2 Мотивация

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

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

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

3 Источники информации

Данные получены из следующих 11 источников.

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

Таблица 2: Источники информации

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

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

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

4 Соотношение Байеса

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

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

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

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

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

где:

B: *соотношение Байеса*

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

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

N: *количество зарегистрированных случаев*

N_a : *среднее количество зарегистрированных случаев в пробном наборе*

C: *вес IP-адреса = 20,000*

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

5 Вычисления

Для каждого источника информации рассчитываются 3 показателя.

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

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

где:

B_m : *максимальное соотношение Байеса*

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

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

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

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

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

где:

N_m : *максимальное количесвто станций в пробном наборе*

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

Индекс для каждого источника данных может быть рассчитан следующим образом:

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

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

Общий НЕ-индекс далее рассчитывается как:

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

где:

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