HostExploit's

World Hosts Report

Март 2013

Вводная часть

Количество вредоносного ПО растет с каждым днем, уровень мастерства киберпреступников также совершенствуется постоянно, но не стоит забывать о том, что каждый сетевой мошенник, существует и в реальном месте и времени. Именно поэтому, развитие хостинг сервисов и повышение стандартов этой отрасли,¬– наиболее актуальная тема сетевой индустрии.

Анализ уровня серверной активности злоумышленников по всему миру с целью оценить их количество, – один из путей такого развития. О 50 наиболее опасных хостингах всего мира, с 2009 года, рассказывает доклад компании HostExploit, WorldHostsReport. Ежеквартальный отчет охватывает более 43 000 автоматизированных систем маршрутизации, собирая данные о зараженных веб-сервисах, бот-сетях, спаме и прочей активности. После сбора информации сопоставляя их с данными от общепризнанных мировых организаций, специализированных на обработке и анализе информации такого рода.

Доклад рассчитан на подготовленную публику, интересующуюся проблематикой: поставщиков сервисов и услуг, специалистов по информационной безопасности, веб-разработчиков, руководителей технических отделов. Конечно, данное исследование оставляет за читателем право сделать собственные выводы, однако факты и цифры говорят сами за себя. Следует подчеркнуть, что большая часть вредоносного контента не была оставлена там специально. Чаще всего его присутствие,– это результат бездействия, а иногда хостинги попросту становятся жертвами злоумышленников. Так например, в этом квартале мы видим возвращение голландского хостинг-провайдера Ecatel на 1 место рейтинга. Несмотря на то, что компания уже попадала в подобную ситуацию несколько раз, данная информация не означает, что Ecatel нацелен на какую-то конкретную активность, через сервера хостинга проходит огромное количество информации

. - Jart Armin

ISBN 978-0-9836249-4-3

Использованные источники

AA419

Abuse.CH

Clean-MX.DE

Cyscon SIRT

Emerging Threats

Google Safe Browsing

Group-IB

HostExploit

hpHosts

ISC

KnujOn

MalwareDomains

MalwareDomainList

RashBL

Robtex

Shadowserver

SiteVet

Spamhaus

SRI International

StopBadware

SudoSecure

Team Cymru

The Measurement Factory

UCE-Protect

Редактор

Jart Armin

Рецензенты

Dr. Bob Bruen

Raoul Chiesa

Peter Kruse

Andre' DiMino

Thorsten Kraft

Andrey Komarov

Godert Jan van Manen

Steven Dondorp

Авторы

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

При сотрудничестве с ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

Northwave

cyscon

SITEVET

ACDC
the Advanced Cyber Defence Centre

Оставайтесь на связи

Если вам нравится то, что мы делаем, и, вы хотите помочь своим участием, станьте нашим спонсором или партнером.

Если вы считаете, что можете быть нам полезны, мы с удовольствием выслушаем ваши предложения. Свяжитесь с нами:

contact@hostexploit.com

Предисловие

Некоторые СМИ Нидерландов уже писали о январском исследовании McAfee, которое поднимало тему глобального распространения ботнет серверов, называя Нидерланды,[1] – «раем для киберпреступников».[2] Мы бы не стали говорить об этом настолько категорично, однако высокий рейтинг активности, в действительности, является постоянной проблемой для этого государства. В рейтинге HostExploit Нидерланды занимают 7 место.

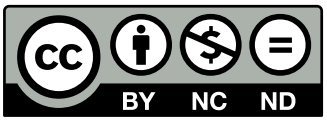
К этой ступени государство привели 2 крупных провайдера, входящих в Топ20: AS29073 Ecatel, занимающая 1 место в мире, и AS16265 LeaseWeb, занимающая 11 строчку рейтинга. В защиту этих компаний можно сказать, что они стали жертвами прекрасной Интернет инфраструктуры Нидерландов. Провайдеры являются безусловными лидерами как на потребительском, так и на корпоративным рынке, оставаясь крупнейшими центрами по передаче трафика.[3]

Эти факты возвращают Ecatel на первое место, которое он занимал уже несколько раз. Хостинг не входит в топ по каким-то конкретным определенным видам активности, через него просто проходит огромное количество данных. Хотелось бы отметить, что в наши цели не входит критика каких-либо конкретных провайдеров, наши результаты предоставляются исключительно с целью ознакомления.

Отказ от ответственности

Мы приложили все усилия, что бы данные, приведенные ниже, на момент публикации были актуальны, а информация была точной, полной и всеобъемлющей. Однако это не означает, что в них могла попасть какая-либо ошибка, связанная ,например, с обновлением или исправлением информации без предварительного уведомления.

HostExploit или какой-либо из наших партнеров, включая CyberDefcon, Group-IB и CSIS, не несет ответственности за неверные и изменённые каким-либо образом данные. Производные выводы и анализ получаемых данных, не может считаться результатом работы HostExploit или кого-либо из наших партнеров.



В случае необходимости использования этого материала свяжитесь CyberDefcon.

1 http://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe
2 http://www.mkbservicedesk.nl/7249/nederland-paradijs-voor-cybercriminelen.htm
3 http://www.rug.nl/news-and-events/people-perspectives/opinie/2013/05mathieupaapst?lang=en

Методология

В 2009 году мы разработали Индекс HE — числовое представление уровня зараженности автономной системы (AC). 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 AC. 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 AC с меньшим адресным пространством, но эта зависимость не линейна. Мы используем «фактор неопределенности» или фактор Баеса, чтобы смоделировать данную функцию, которая повышает значения для AC 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.

Определения и уточнения

IPs

В данном отчете поле «IPs» относится к числу зарегистрированных IPv4 адресов выделенных AC.В контексте конкретных стран, это общая сумма «IPs» для AS этой страны.

Страны

С того момента как AC начали физически маршрутизироваться через несколько стран, HostExploit определяет страны на основе их регистрационных данных и расположении маршрутизаторов.

Индекс HE

Количественные данные HostExploit показывают концентрацию вредоносной активности, полученную во время анализа Автономных Систем.

Рейтинг HE

Рейтинг индекса в сравнении со всеми 43,454 анализируемыми Автономными Системами.

Более подробную информацию вы можете увидеть в разделе Глоссарий.

ТОП 50

Рейтинг 50 АС с наиболее высоким индексом HE и с самой высокой вредоносной активностью.

Автономная система (АС)

Логичное собрание Интернет маршрутов, контролируемых какой-либо организацией или ISP.

ASN

Уникальный порядковый номер АС.

Индекс HE

Количественные данные HostExploit показывают концентрацию вредоносной активности, полученную во время анализа Автономных Систем.

Рейтинг HE

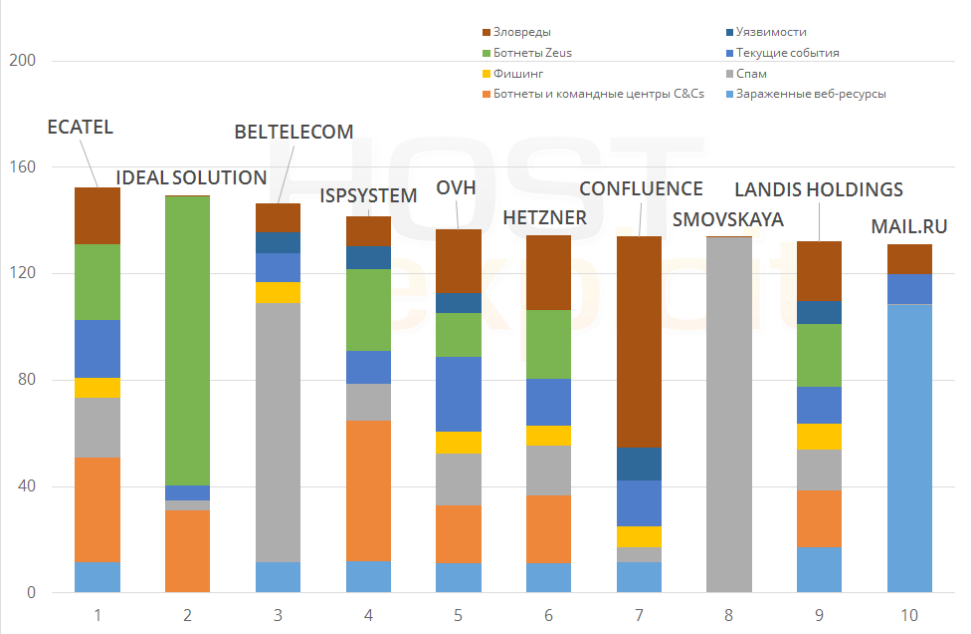
Рейтинг индекса в сравнении со всеми 43,454 анализируемыми Автономными Системами.

IPs

Количество адресов Интернет Протокола приписанных к одной АС.

Рейтинг HE	Индекс HE	ASN	Название АС	Страна АС	IPs
1	152.38	29073	Ecatel Network	NL	13,056
2	149.22	58001	Ideal Solution Ltd	RU	2,304
3	146.69	6697	Beltelecom	BY	1,420,800
4	141.69	29182	ISPsystem	RU	44,800
5	136.65	16276	OVH Systems	FR	1,003,008
6	134.49	24940	Hetzner Online AG	DE	638,208
7	133.96	40034	Confluence Networks Inc	VG	11,776
8	133.83	197774	Smovskaya Valentina Ivanovna	UA	512
9	132.18	11042	Landis Holdings Inc	US	28,416
10	131.11	47764	Mail.Ru LLC	RU	25,088
11	130.72	16265	LeaseWeb B.V.	NL	349,184
12	130.65	51699	Antarktida-Plus	SC	256
13	130.35	47781	"Delta-X" Ltd	UA	1,536
14	129.30	33182	HostDime.com, Inc.	US	55,040
15	128.05	4134	Chinanet Backbone	CN	116,912,864
16	126.03	32475	SingleHop	US	321,024
17	125.66	36351	SoftLayer Technologies Inc.	US	1,329,408
18	125.46	23535	HostRocket	US	13,312
19	124.07	50465	IQHost Ltd	RU	2,304
20	123.64	8560	1&1 Internet AG	DE	370,688
21	120.94	39743	Voxility S.R.L.	RO	29,696
22	119.63	12824	home.pl	PL	204,800
23	116.12	26347	New Dream Network, LLC	US	219,648
24	114.39	31034	Aruba S.p.A.	IT	140,800
25	111.89	38731	Vietel - CHT Compamy Ltd	VN	31,488
26	111.42	198354	SIS Laboratory, LLC	RU	3,328
27	109.94	26496	GoDaddy.com, LLC	US	1,610,496
28	109.47	22489	Castle Access Inc	US	48,384
29	108.73	8342	OJSC RTComm.RU	RU	463,872
30	108.21	9891	CS Loxinfo	TH	20,992
31	106.82	46475	Limestone Networks, Inc.	US	86,016
32	106.69	27823	Dattatec.com	AR	8,192
33	106.17	4837	China169 Backbone	CN	53,791,744
34	104.66	49467	Internet Hizmetleri (izmir)	TR	11,264
35	104.55	21844	ThePlanet.com Internet Services	US	1,509,376
36	100.93	9198	Kazakhtelecom	KZ	2,445,056
37	100.06	44112	SpaceWeb JSC	RU	3,584
38	99.41	51559	Netinternet	TR	17,664
39	98.72	46606	Unified Layer	US	235,520
40	97.61	23352	Server Central Network	US	259,584
41	95.49	13147	NetInfo Ltd.	BG	8,704
42	95.43	9931	The Communication Authoity of Thailand	TH	212,480
43	95.08	34109	CB3ROB Ltd.	DE	9,216
44	94.95	55660	PT Master Web Network	ID	4,096
45	94.29	49335	Navitel Rusconnect Ltd	RU	12,544
46	94.05	32613	iWeb Technologies Inc.	CA	251,904
47	93.80	20773	Host Europe GmbH	DE	220,672
48	93.40	21219	Datagroup	UA	132,864
49	92.22	20454	Secured Servers LLC	US	90,880
50	91.42	12322	PROXAD Free SAS	FR	12,271,616

График распределения Индекса НЕ



Что это?

Диаграмма слева дает визуальное представление, какой вклад каждый сектор вносит в значение индекса.

Это позволяет вам быстро увидеть, где конкретно стоит улучшить узел.

ТОП 10 Новичков

Рейтинг 10 АС с наиболее высоким рейтингом среди всех 2,195 АС зарегистрированных с момента выпуска последней версии исследования. Эта информация может быть интересна для дальнейших наблюдений.

Рейтинг НЕ	Индекс НЕ	ASN	Название АС	Страна АС	IPs
88	76.2	61421	Astra LLC.	RU	256
274	55.0	61322	Sotal-Interactive ZAO	RU	256
343	49.7	56598	KartLand Ltd.	RU	256
447	43.4	22611	InMotion Hosting, Inc.	US	16,128
522	40.9	20785	ISP UCT	UA	256
673	35.2	132322	Good Domain Registry	IN	1,024
740	33.4	33667	Comcast Cable Communications	US	0
1,210	23.7	17589	Gabia Inc.	KR	30,720
1,261	22.8	59684	Hoster kg, Ltd.	KG	1,024
1,351	21.7	61387	Denkers-ICT B.V.	NL	1,536

Количество АС

в 3 квартале 2012
42,386

В этом отчтете
43,454

Новые АС
2,195

Удаленные
1,127

увеличение
1,068

Что это?

Мы рассчитываем индекс для каждой страны, используя одинаковый метод для каждой АС.

Индекс страны засчитывается в случае превышения уровня вредносной активности в 1,000 пунктов, без привязки к количеству хостов.

В правой таблице можно увидеть топ 10 стран, рассчитаных с помощью данного методу, также показаны 3 сектора с наиболее высокими индексами.

Топ 10 стран

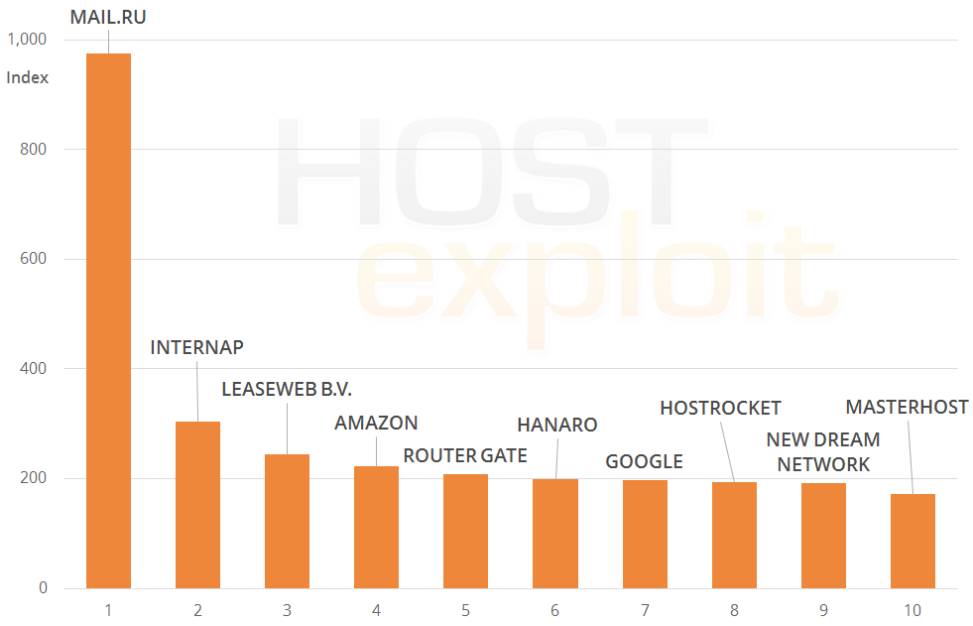
Страна АС	Название АС	ASes	IPs	Рейтинг	Индекс
RU	RUSSIAN FEDERATION	4,090	54,994,464	1	391.2
	Highest sector		Infected web sites	1	933.3
	2nd-highest sector		Badware	1	618.8
	3rd-highest sector		Botnet C&Cs	2	445.8
BY	BELARUS	79	2,167,808	2	265.0
	Highest sector		Spam	1	762.8
	2nd-highest sector		Infected web sites	3	475.4
	3rd-highest sector		Phishing	7	148.0
UA	UKRAINE	1,673	15,085,184	3	252.4
	Highest sector		Botnet C&Cs	3	433.2
	2nd-highest sector		Zeus botnets	6	386.5
	3rd-highest sector		Spam	2	359.9
VG	VIRGIN ISLANDS, BRITISH	4	17,152	4	220.8
	Highest sector		Exploits	1	902.7
	2nd-highest sector		Badware	2	417.6
	3rd-highest sector		Infected web sites	9	371.1
US	UNITED STATES	14,632	1,251,674,571	5	217.8
	Highest sector		Infected web sites	11	307.6
	2nd-highest sector		Badware	5	244.4
	3rd-highest sector		Zeus botnets	12	218.3
RO	ROMANIA	1,068	13,610,752	6	215.3
	Highest sector		Infected web sites	4	433.5
	2nd-highest sector		Zeus botnets	7	375.3
	3rd-highest sector		Botnet C&Cs	5	237.6
NL	NETHERLANDS	517	58,569,794	7	202.8
	Highest sector		Infected web sites	2	557.7
	2nd-highest sector		Badware	7	217.0
	3rd-highest sector		Botnet C&Cs	8	192.4
PL	POLAND	1,542	21,701,696	8	194.4
	Highest sector		Infected web sites	8	389.7
	2nd-highest sector		Exploits	4	354.0
	3rd-highest sector		Badware	6	235.9
TR	TURKEY	297	21,354,240	9	189.0
	Highest sector		Infected web sites	7	396.3
	2nd-highest sector		Badware	3	332.4
	3rd-highest sector		Phishing	6	169.6
BG	BULGARIA	449	5,647,872	10	186.0
	Highest sector		Zeus botnets	8	363.0
	2nd-highest sector		Badware	4	312.5
	3rd-highest sector		Botnet C&Cs	4	303.4

Зараженные веб-ресурсы

Индекс	ASN	Название АС	Страна АС	IPs	Рейтинг НЕ	Индекс НЕ
975.7	47764	Mail.Ru LLC	RU	25,088	10	131.1
304.7	14744	Internap Network Services	US	124,928	185	63.3
244.9	16265	LeaseWeb B.V.	NL	349,184	11	130.7
222.2	16509	Amazon.com, Inc.	US	2,125,568	117	71.4
208.3	43260	Router Gate	TR	14,848	128	69.5
199.8	9318	Hanaro Telecom	KR	15,072,512	54	90.3
197.6	15169	Google Inc.	US	667,136	64	84.9
193.6	23535	HostRocket	US	13,312	18	125.5
191.8	26347	New Dream Network, LLC	US	219,648	23	116.1
171.4	25532	Masterhost	RU	77,824	123	69.8

Количество вредоносных URL на серверах Mail.ru резко возросла за последний квартал, их подавляющее большинство распространяется с серверов файл хостинга и менеджера загрузок. Этот рост стал главным фактором попадания компании в Топ 10. Такое резкое увеличение вредоносных файлов могло произойти из-за введения новых функций, изменения в политике безопасности или атаки киберпреступников, которые выбрали хостинги Mail.ru в качестве временного хранилища.

С другой стороны можно заметить рост рейтинга компании HostRocket, который заметно прослеживается в течение последних двух кварталов. Высокий рейтинг в категории инфицированных веб-сайтов и зловредного ПО говорит о том, что проблема кроется в хранящимся на серверах контенте.



Знаете ли вы?

Знаете ли вы, что компания Hanaro Telecom, находящаяся на 54 месте занимает самый высокий рейтинг активности среди корейских АС.

Сухие цифры

Более 59% зараженных URL-адресов хранятся на серверах компаний, входящих в Топ 10.

Знаете ли вы?

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

Ботнеты и командные центры C&Cs

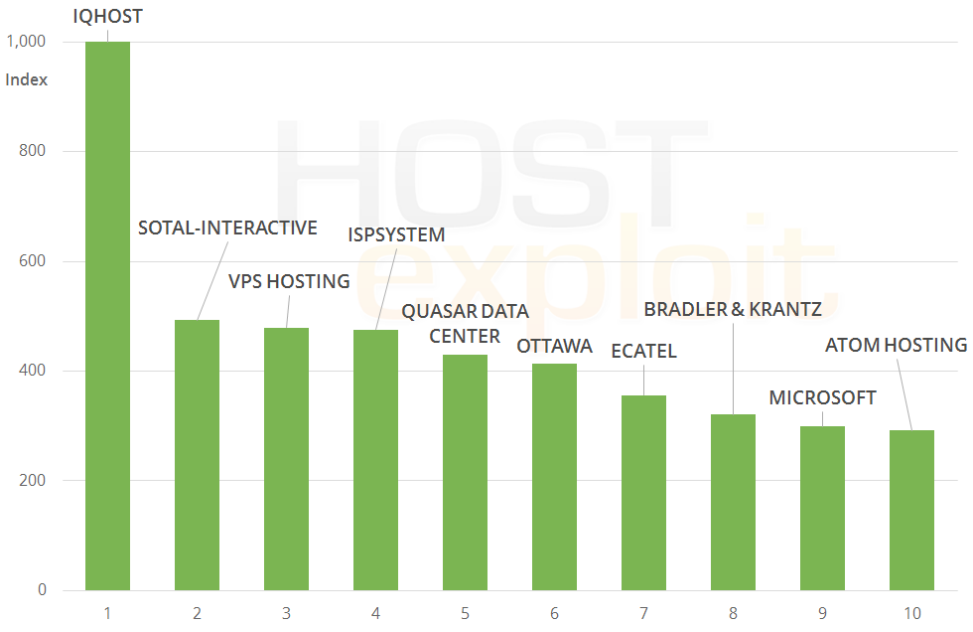
Индекс	ASN	Название AC	Страна AC	IPs	Рейтинг HE	Индекс HE
1,000.0	50465	IQHost Ltd	RU	2,304	19	124.1
492.5	61322	Sotal-Interactive ZAO	RU	256	274	55.0
479.6	56617	SIA "VPS Hosting"	LV	1,024	171	64.4
475.4	29182	ISPsystem	RU	44,800	4	141.7
430.1	46785	Quasar Data Center, Ltd.	US	4,608	241	58.2
413.3	26230	Telecom Ottawa Limited	CA	22,272	387	46.9
356.0	29073	Ecatel Network	NL	13,056	1	152.4
321.0	29141	Bradler & Krantz GmbH	DE	19,456	191	62.6
298.6	8069	Microsoft Corp	US	0	350	49.4
292.0	13209	Atom Hosting SRL	RO	768	233	58.9

Наиболее заметным в десятке Ботнетов и их командных центров является «Sotal-Interactive», который был вновь зарегистрирован в последнем квартале. С количественным значением в 256 IPs (минимум для AC), несмотря на наибольшую аткивность в России, эта сеть зарегистрирована в Украине. Злоумышленникам, похоже, удалось подогнать профиль Настройки AC для одноразовых ботнетов.

Интерес представляет включение в список одной из AC Microsoft, несмотря на отсутствие объявлений о каких-либо IP блокировках. По всей видимости, это вопрос времени, этот командный центр был впервые обнаружен в 2012 году, когда блокировка a\16 был передана этому AC, на последнее объявление, кстати, не было никакой реакции.

Сухие цифры

Активность всех 132 Командных Центров в последнем квартале была чуть меньше, нежели чем вредоносная активность любой другой категории. Однако мощь подобных сетей, подчеркивает важность их изучения и анализа с точки зрения безопасности.

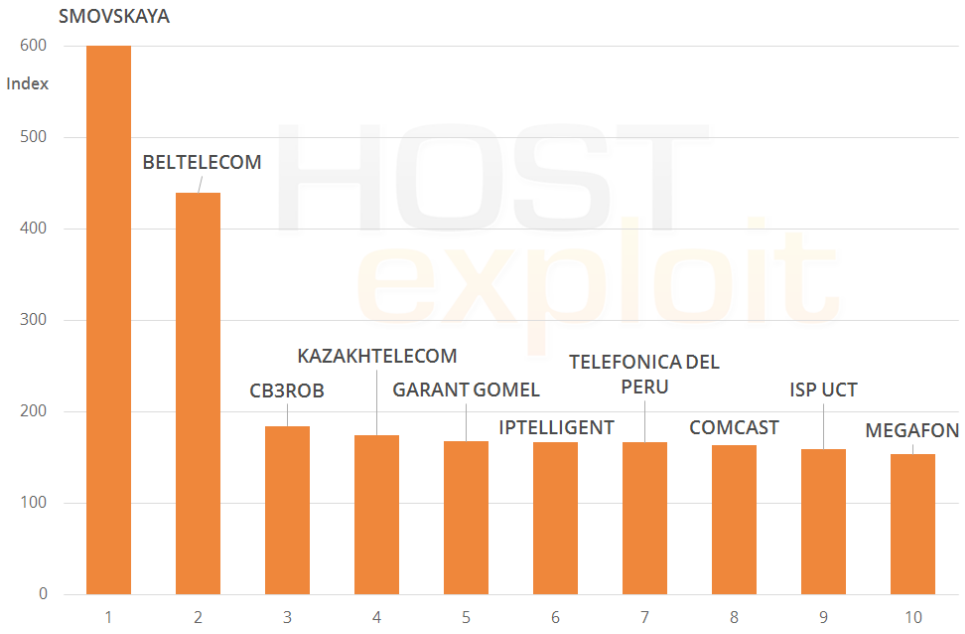


Спам

Индекс	ASN	Название АС	Страна АС	IPs	Рейтинг НЕ	Индекс НЕ
601.8	197774	Smovskaya Valentina Ivan...	UA	512	8	133.8
439.3	6697	Beltelecom	BY	1,420,800	3	146.7
184.1	34109	CB3ROB Ltd.	DE	9,216	43	95.1
174.6	9198	Kazakhtelecom	KZ	2,445,056	36	100.9
167.2	42036	Garant Gomel	BY	7,936	613	37.2
167.0	8100	IPTelligent LLC	US	47,104	169	64.8
166.5	6147	Telefonica del Peru	PE	1,976,576	244	57.9
163.7	20214	Comcast Cable	US	256	375	47.3
158.6	20785	ISP UCT	UA	256	522	40.9
153.3	31133	OJSC MegaFon	RU	29,184	110	73.2

В предыдущих докладах тенденция прослеживалась однозначно: спамеры предпочитают посылать свою почту из стран, где уровень регулирования, настройки и правовых норм необходимых для регистрации АС, чрезвычайно низкий. Таким образом, мы могли наблюдать некое доминирование в Топ10, среди хостинг-сервисов из Индии, Пакистана и Вьетнама. В последнем квартале, например, половина хостов из верхней десятки были зарегистрированы в Индии.

Однако, в этом квартале нету такого доминирования со стороны индийцев в Топ 10. Вместо этого в верхней десятке, мы видим микс из небольших, специально построенных под спам серверов («Smovskaya» и недавно зарегистрированный ISP UCT, оба в Украине) и крупных телекоммуникационных компаний, которые продолжают бороться со спам-активностью: Belttelecom, Казахтелеком и и Telefonica Del Peru.



Что мы собираемся сделать?

В этой категории мы рассмотрим традиционные спам сервера, а также спам-ботов, сканеры и репутацию общественных IP.

Знаете ли вы?

В нашем докладе за первый квартал 2012 года у Мегафона насчитывалось 4 АС в Топ10, посвященной спаму.

Сухие цифры

В последнем квартале были рассмотрены и проанализированы более 100,000 источников спама.

Знаете ли вы?

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

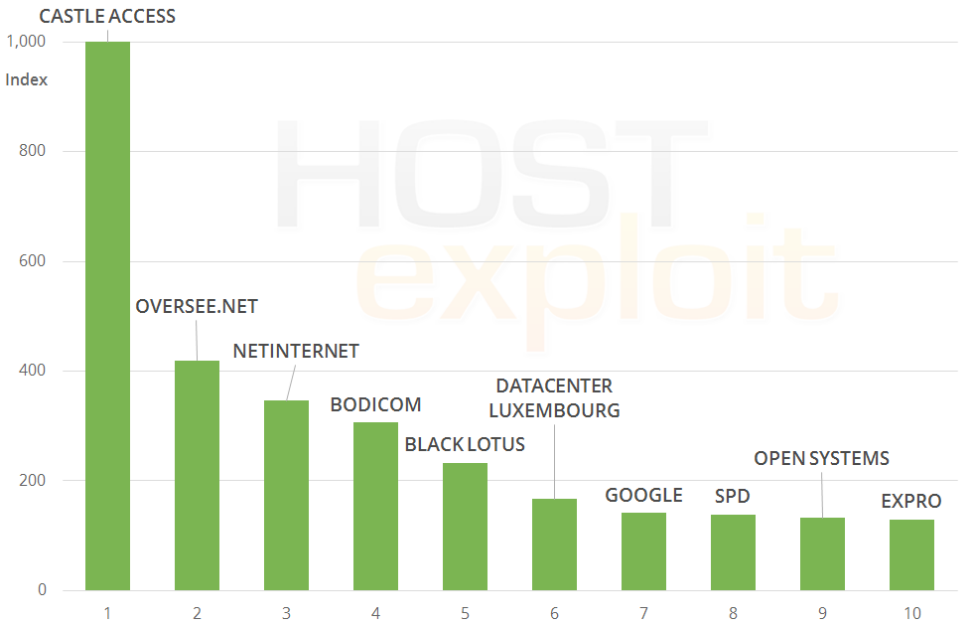
Фишинг

Индекс	ASN	Название AC	Страна AC	IPs	Рейтинг HE	Индекс HE
1,000.0	22489	Castle Access Inc	US	48,384	28	109.5
419.4	33626	Oversee.net	US	3,584	113	72.6
346.2	51559	Netinternet	TR	17,664	38	99.4
305.9	45237	Bodicom ISP Ulaanbaatar	MN	5,120	561	39.1
232.7	32421	Black Lotus Communic...	US	11,264	787	31.6
166.2	24611	Datacenter Luxembourg	LU	8,704	3,168	12.6
141.5	15169	Google Inc.	US	667,136	64	84.9
139.0	40028	Spd Network	CA	17,664	1,196	24.0
132.7	28721	Open Systems S.R.L.	RO	2,560	3,034	13.4
129.8	31199	Expro Sp. z o.o.	PL	512	2,496	15.5

Фишинг — один из наиболее быстро развивающихся направлений киберпреступности. Это подчеркивается тем фактом, что большинство фишинг-сайтов могут подключаться всего на несколько минут. По этой причине лишь один из такого рода опасных сервисов оказался в десятке. Не стоит забывать и о коротком веке подобного рода веб-ресурсов. Кстати этот факт подчёркивает необходимость для злоумышленников регистрировать их на хостингах США и Канады, где конечно более строиге условия регистрации, но при этом сервис позволяет быстро отключить страницу.

Сухие цифры

В предыдущем квартале, в общей сложности 110 случаев фишинга были зарегистрированы на этих 10 узлах, из общих 2461 фишинг-атаки за квартал.

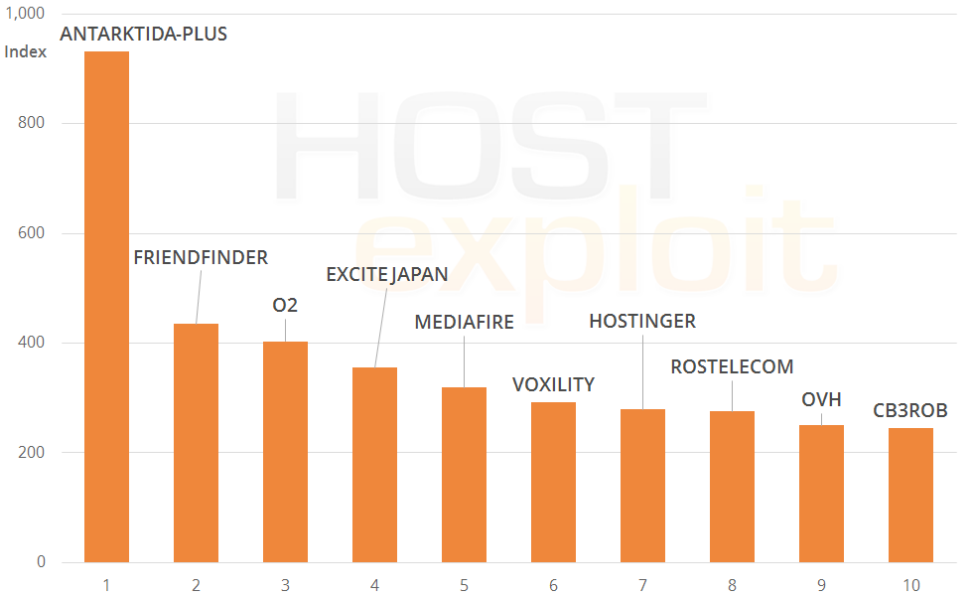


Текущие события

Индекс	ASN	Название АС	Страна АС	IPs	Рейтинг НЕ	Индекс НЕ
931.6	51699	Antarktida-Plus	SC	256	12	130.7
434.7	32527	FriendFinder Networks	US	2,560	359	48.6
402.7	31080	o2 Sp. Z.o.o.	PL	512	329	50.8
355.0	45682	Excite Japan Co., Ltd.	JP	2,048	549	39.8
318.8	46179	MediaFire, LLC	US	3,072	511	41.1
291.4	39743	Voxility S.R.L.	RO	29,696	21	120.9
279.2	47583	Hostinger International	US	6,144	101	74.8
275.8	35177	Rostelecom	RU	32,768	270	55.2
250.1	16276	OVH Systems	FR	1,003,008	5	136.7
244.5	34109	CB3ROB Ltd.	DE	9,216	43	95.1

Как и предполагает название, этот раздел представляет собой быстроменяющийся сектор, который представляет из себя различные типы вредоносных активнсотей ,размещаемых на разных хостах. С момента последней пубикации из таких активностей только Voxility остался в Топ10. Из крупных и общеизвестных игроков здесь были отмечены FriendFinder и MediaFire, а также большой французский веб-хостинг компании, OVH.

Также было замечено, что три АС были зарегистрированы в стране отличной от их размещения: Antarktida в России, Hostinger в Литве и CB3ROB в Нидерландах.



Знаете ли вы?

«Текущие события» HostExploit – это исследование самых современных и быстроменяющихся атак со всего мира.

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

Сухие цифры

The number of Current Events instances observed over the reporting period was less than 17% of the instances during the previous period.

Знаете ли вы?

Как форма ботнета Zeus попадает на зараженные машины как троянец полезной нагрузки. Этот вирус остается одним из самых популярных сортов ботнет, не смотря на то, что популярность в андерграудных кругах преступников он получил около 5 лет назад.

Zeus постоянно улучшает свою структуру, и имеет много ее вариаций, каждая из которых старается обойти системы безопасности и превратить в «зомби» максимальное количество машин.

Ботнеты Zeus

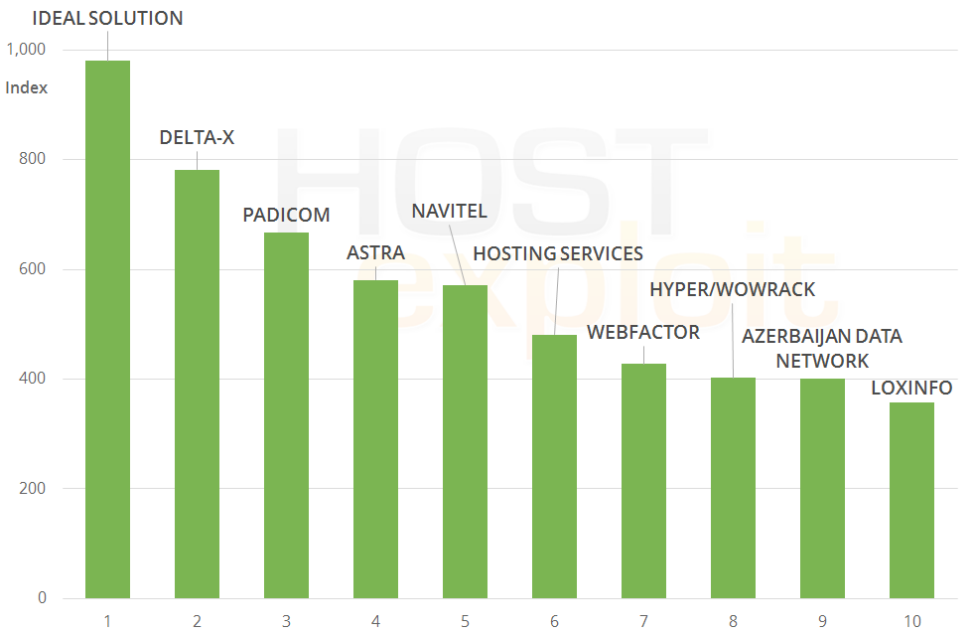
Индекс	ASN	Название AC	Страна AC	IPs	Рейтинг HE	Индекс HE
980.1	58001	Ideal Solution Ltd	RU	2,304	2	149.2
781.5	47781	"Delta-X" Ltd	UA	1,536	13	130.4
667.0	34201	Padicom Solutions SRL	RO	6,400	104	74.4
580.6	61421	Astra LLC.	RU	256	88	76.2
571.3	49335	Navitel Rusconnect Ltd	RU	12,544	45	94.3
481.4	29302	Hosting Services Inc	GB	6,144	83	77.3
427.8	35818	Webfactor SRL	RO	11,008	52	90.8
401.9	23033	Hyper to Wowrack	US	35,328	89	76.2
399.9	15621	Azerbaijan Data Network	AZ	14,336	257	56.6
357.7	9891	CS Loxinfo	TH	20,992	30	108.2

Ideal Solution, сеть зарегистрированная на Сейшельских островах, поднялась с #9 на #1 место среди Зевс-ботнетов.

Рейтинг этого зловреда поднялся до 4 места. Также следует отметить появление LCC ASTRA,– недавно зарегистрированный российский ботнет, который сразу же поднялся прямо на #4 места. Также выделены 2 командных центра Zeus с 256 IPs. Стоит отметить, что 8 из 10 AC базируются в Восточной Европе, эти данные не изменились по сравнению с прошлым отчетом.

Сухие цифры

Общее количество серверов Zeus за год практически не изменилось. Как только специалистам удается обрушить командный центр ботнета, он появляется снова в каком-либо другом месте.

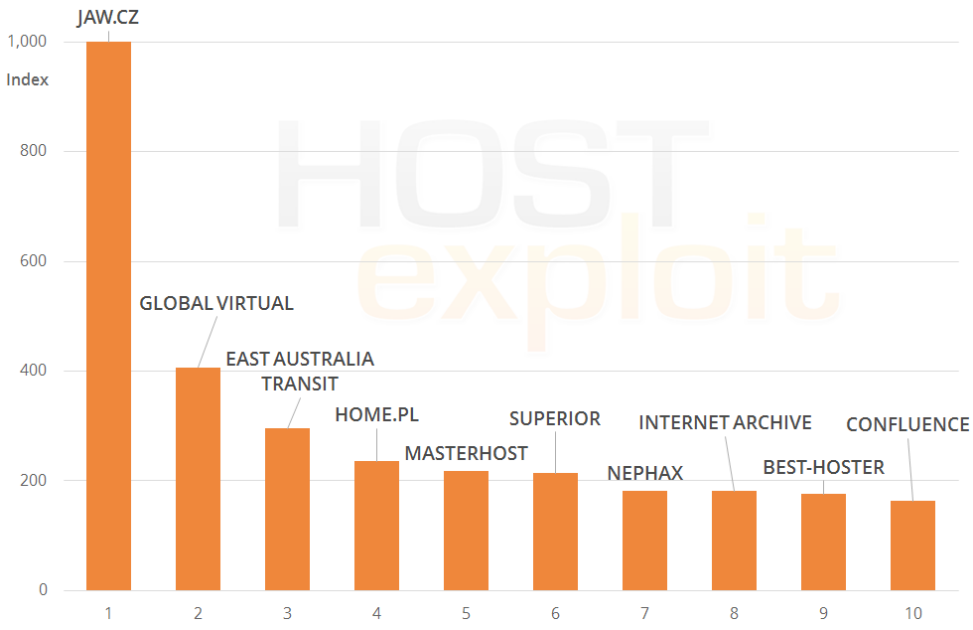


Уязвимости

Индекс	ASN	Название AC	Страна AC	IPs	Рейтинг HE	Индекс HE
1,000.0	43070	JAW.cz s.r.o.	CZ	3,584	73	81.5
406.9	46549	Global Virtual Opportunities	US	3,584	60	86.7
295.6	45261	East Australia Transit	AU	82,688	712	34.4
235.2	12824	home.pl	PL	204,800	22	119.6
217.6	25532	Masterhost	RU	77,824	123	69.8
213.8	34233	Superior B.V.	NL	4,096	330	50.6
181.5	43333	CIS NEPHAX	PL	17,920	326	50.9
181.0	7941	Internet Archive	US	6,144	449	43.4
175.6	49693	Best-Hoster Group Co. Ltd	RU	1,024	334	50.4
163.1	40034	Confluence Networks Inc	VG	11,776	7	134.0

Несмотря на снижение в общем рейтинге,ПО такого рода со 2 место упало до 7, уязвимость Confluence Network в Топ-10. Число, проаналищированных на JAW.cz эксплойтов, сильно увеличилось быстро, подняв свой индекс со 109,3 пунтков до максимальной 1,000.0. Этого роста было достаточно для подъема в общем рейтинге с #4,758 на #73 место.

Home.pl остался в Топ10 всех уязвимостей. Учитывая роль ПО в фишинговых атаках, зловред успешно стремится к #22 месту.



Знаете ли вы?

Уязвимости и веб-сервисы, работающие для их распространения являются ключевой частью головоломки всех киберпреступлений.

Чаще всего именно с их помощью злоумышленники взламывают компьютеры своих жертв. Уязвимости ищут брешь в программном обеспечении, используя поддельный код, который непосредственно подрывает систему жертвы, и передает бразды правления машиной мошенникам.

Сухие Цифры

Топ 10 AC в этой категории отвечают за более чем 29% всех уязвимостей замеченных в период подготовки исследования.

Знаете ли вы?

Вредоносное программное обеспечение принципиально игнорируется пользователями во время работы на своих машинах. Примеры такого программного обеспечения включают spyware, некоторые виды malware, rouge и обманного adware. Последний обычно появляется в виде заставки, требующей обновления при нажатии на кнопку перекидывают пользователя на страницы с кей-логгером, который крадет личные данные.

Сухие Цифры

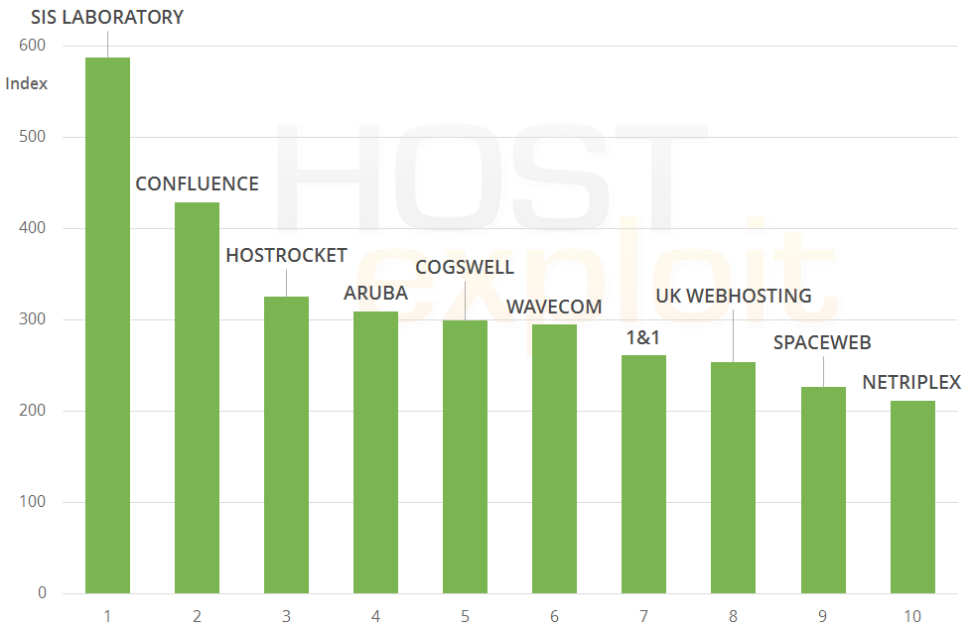
Общий показатель всех наблюдаемых зловредов упал более чем на 65% по сравнению с предыдущим кварталом. Отчасти это можно объяснить окончанием праздничных каникул во всем мире.

Зловреды

Индекс	ASN	Название AC	Страна AC	IPs	Рейтинг HE	Индекс HE
587.1	198354	SIS Laboratory, LLC	RU	3,328	26	111.4
429.0	40034	Confluence Networks Inc	VG	11,776	7	134.0
325.2	23535	HostRocket	US	13,312	18	125.5
308.6	31034	Aruba S.p.A.	IT	140,800	24	114.4
299.0	19066	Cogswell Enterprises Inc.	US	41,984	53	90.6
294.9	34702	WaveCom AS	EE	9,216	103	74.5
261.2	8560	1&1 Internet AG	DE	370,688	20	123.6
254.1	35732	UK Webhosting Ltd	GB	4,096	58	87.3
226.1	44112	SpaceWeb JSC	RU	3,584	37	100.1
211.9	36167	Netriplex LLC	US	1,536	464	43.1

Вся 10 AC в этой категории изменилась с момента предыдущего квартала.Это говорит о том: что преступники быстро приспасабливаются и постоянно придумывают что-то новое, изменения в этом секторе также протекают очень быстро. Также это говорит о том, что активность преступников с точки зрения ПО чаще всего сезонна,– наиболее печально известные вирусы активно распространялись именно во время праздников.

Половина из узлов в Топ 10 также попали в Топ-100 рейтинга по фишинг-угрозам и зараженным веб-сайтам . Такое соотношение получается из-за схожести требования хостинга для всех 3 секторов.



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)*