



Kaspersky Security Bulletin

Основная статистика за
2009 год

Александр Гостев
Евгений Асеев

КАСПЕРСКИЙ lab

Вредоносные программы в интернете

<u>(атаки через Web)</u>	<u>3</u>
<u>Вредоносные программы в интернете: TOP-20</u>	<u>4</u>
<u>Страны, на ресурсах которых размещены</u>	
<u>вредоносные программы: TOP-20</u>	<u>5</u>
<u>Страны, в которых пользователи подвергались</u>	
<u>атакам в 2009 году: TOP-20</u>	<u>7</u>
<u>Сетевые атаки</u>	<u>8</u>
<u>Локальные заражения</u>	<u>10</u>
<u>Уязвимости</u>	<u>12</u>

Отчет сформирован на основе данных, полученных и обработанных при помощи Kaspersky Security Network. KSN является одним из важнейших нововведений в персональных продуктах и в настоящее время готовится к включению в состав корпоративных продуктов «Лаборатории Касперского».

Kaspersky Security Network позволяет нашим экспертам оперативно, в режиме реального времени, обнаруживать новые вредоносные программы, для которых еще не существует сигнатурного или эвристического детектирования. KSN позволяет выявлять источники распространения вредоносных программ в интернете и блокировать доступ пользователей к ним.

Одновременно KSN позволяет реализовать значительно большую скорость реакции на новые угрозы – в настоящее время мы можем блокировать запуск новой вредоносной программы на компьютерах пользователей KSN через несколько десятков секунд с момента принятия решения о ее вредоносности, и это осуществляется без обычного обновления антивирусных баз.

Вредоносные программы в интернете (атаки через Web)

В основной части отчета мы уделили значительное внимание проблеме веб-эпидемии Gumblog. На самом деле эта эпидемия является только верхушкой айсберга веб-инфекций, которые на протяжении последних лет стали доминирующим способом заражения компьютеров пользователей.

В этой области киберпреступность достаточно быстро эволюционировала, выйдя на уровень создания полноценных ботнетов из взломанных веб-сайтов, способных самостоятельно поддерживать свою популяцию.

Кроме того, активно используются возможности, предоставляемые социальными сетями. Наши наблюдения показывают, что существующий уровень доверия между пользователями социальных сетей является очень высоким. Вероятность того, что пользователь социальной сети запустит предлагаемый ему «друзьями» файл или пройдет по присланной от имени «друга» ссылке примерно в 10 раз выше, чем если бы этот файл или ссылка пришли к нему по электронной почте. И злоумышленники используют это при распространении вредоносных программ и спама.

Мы неоднократно писали о технологии drive-by-download. При ее использовании заражение компьютера происходит незаметно для пользователя во время обычной работы в интернете. В 2009 году ситуация значительно ухудшилась – число подобных атак, зафиксированных нами, увеличилось примерно в 3 раза. При этом следует понимать, что речь идет о десятках миллионов атак.

При помощи Kaspersky Security Network мы можем осуществлять учет и ана-

лиз всех попыток заражения наших пользователей при работе в интернете.

По итогам работы KSN в 2009 году зафиксировано 73 619 767 (аналогичный показатель 2008 года - 23 680 646) атак на наших пользователей, которые были успешно отражены. Кроме попыток загрузки на компьютеры вредоносных и потенциально опасных программ в число зафиксированных инцидентов вошли 14 899 238 попыток доступа к фишинговым и вредоносным сайтам, которые были заблокированы нашим антивирусом.

Вредоносные программы в интернете: TOP-20

Из всех вредоносных программ, участвовавших в интернет-атаках на пользователей, мы выделили 20 наиболее активных. Каждая из этих 20 угроз была зафиксирована нами более 170 000 раз, на них пришлось более 37% (27 268 356) всех зафиксированных инцидентов.

	Название	Количество атак	% от общего
1	HEUR:Trojan. Script.Iframer	9858304	13,39
2	Trojan- Downloader. JS.Gumblar.x	2940448	3,99
3	not-a- virus:AdWare. Win32.Boran.z	2875110	3,91
4	HEUR:Exploit. Script.Generic	2571443	3,49
5	HEUR:Trojan- Downloader. Script.Generic	1512262	2,05
6	HEUR:Trojan. Win32.Generic	1396496	1,90
7	Worm.VBS. Autorun.hf	1131293	1,54
8	Trojan- Downloader. HTML.IFrame.sz	935231	1,27
9	HEUR:Exploit. Script.Generic	752690	1,02
10	Trojan. JS.Redirector.l	705627	0,96
11	Packed.JS.Agent. bd	546184	0,74
12	Trojan-Clicker. HTML.Agent.aq	379872	0,52

	Название	Количество атак	% от общего
13	HEUR:Trojan-Downloader. Win32.Generic	322166	0,44
14	Trojan.JS.Agent.aat	271448	0,37
15	Trojan-Downloader. Win32.Small.aacq	265172	0,36
16	Trojan-Clicker. HTML.IFrame.ani	224657	0,31
17	Trojan-Clicker. JS.Iframe.be	216738	0,30
18	Trojan-Downloader. JS.Zapchast.m	193130	0,27
19	not-a-virus:AdWare. Win32. GamezTar.a	170085	0,23
	Всего TOP20	27268356	37,06

Первое место в рейтинге со значительным отрывом занимает эвристическое детектирование вредоносных ссылок, которые внедряются хакерами, а зачастую и самими вредоносными программами, в код взломанных сайтов. Эти ссылки осуществляют скрытое обращение браузера к другому сайту, на котором, как правило, и находится основной набор эксплоитов, использующих уязвимости браузеров и приложений.

Второе место досталось Gumblar, и это не удивительно, учитывая размах его эпидемии. Почти 3 000 000 раз наш продукт детектировал обращения наших клиентов к серверам данного ботнета. Можно только вообразить себе, сколько миллионов персональных компьютеров могли бы стать жертвами этой вредоносной программы.

Примечательно и то, что третье место заняла рекламная программа Boran.z. Adware уже давно является, наряду со спамом и порнографией, одним из основных движущих элементов в структуре киберпреступности.

Практически все остальные участники двадцатки в той или иной мере относятся к различным вариациям эксплоитов уязвимостей.

Страны, на ресурсах которых размещены вредоносные программы: TOP-20

73 619 767 атак, зафиксированных нами в 2009 году, проводились с интернет-ресурсов, размещенных в 174 странах мира. Более 97% всех зафиксирован-

ных нами атак было осуществлено из двадцати стран.

1	CHINA (mainland)	52,70%
2	UNITED STATES	19,02%
3	NETHERLANDS	5,86%
4	GERMANY	5,07%
5	RUSSIAN FEDERATION	2,58%
6	UNITED KINGDOM	2,54%
7	CANADA	2,22%
8	UKRAINE	2,17%
9	LATVIA	1,53%
10	FRANCE	0,60%
11	SPAIN	0,49%
12	South KOREA	0,48%
13	BRAZIL	0,44%
14	CYPRUS	0,34%
15	SWEDEN	0,32%
16	TAIWAN	0,27%
17	NORWAY	0,23%
18	ISRAEL	0,21%
19	LUXEMBOURG	0,16%
20	ESTONIA	0,16%
		97,38%

Первая пятерка стран в таблице идентична первой пятерке в аналогичном рейтинге 2008 года.

Как и год назад, абсолютным лидером по числу атак, проведенных с ресурсов, размещенных в стране, стал Китай. Однако процент атак, проведенных с китайских веб-ресурсов, уменьшился с 79% до почти 53%. На втором месте по-прежнему США, при этом доля зараженных серверов на территории этой страны значительно выросла – с 6,8% до 19%. Россия, Германия и Голландия составляют «второй эшелон», и их доли выросли незначительно.

Лидерство Китая, как в области создания новых вредоносных программ, так и по числу зараженных веб-сайтов, уже стало объектом внимания со стороны правительственных и правоохранительных органов страны. Для исправления ситуации регулирующие органы уже предприняли ряд мер, призванных усложнить появление вредоносных ресурсов. Теперь оформление доменного имени в зоне .cn производится по письменному заявлению установленного образца и только после того, как заявитель лично предъявит удостоверение и лицензию на осуществление коммерческой деятельности. Из-за несоблюдения этих норм уже были закрыты несколько китайских компаний-регистраторов доменов.

Практически сразу после введения (в конце 2009 года) данных мер было отмечено уменьшение числа ссылок на китайские домены в спаме. Мы надеемся,

что в 2010 году эта же тенденция затронет и прочие способы заражения компьютеров и обмана пользователей.

Страны, в которых пользователи подвергались атакам в 2009 году: TOP-20

Следующий показатель, требующий рассмотрения: пользователи каких стран и регионов стали объектами атак.

Более 86% из 73 619 767 зафиксированных попыток заражения пришлось на компьютеры жителей следующих двадцати стран:

1	CHINA (mainland)	46,75%
2	UNITED STATES	6,64%
3	RUSSIAN FEDERATION	5,83%
4	INDIA	4,54%
5	GERMANY	2,53%
6	UNITED KINGDOM	2,25%
7	SAUDI ARABIA	1,81%
8	BRAZIL	1,78%
9	ITALY	1,74%
10	VIET NAM	1,64%
11	MEXICO	1,58%
12	FRANCE	1,49%
13	EGYPT	1,37%
14	TURKEY	1,23%
15	SPAIN	1,20%
16	UKRAINE	0,91%
17	CANADA	0,81%
18	MALAYSIA	0,80%
19	THAILAND	0,76%
20	KAZAKHSTAN	0,71%
		86,37%

По сравнению с прошлым годом в этом рейтинге произошли значительные изменения. Китай по-прежнему лидирует по числу потенциальных жертв, но его доля уменьшилась на 7%. А вот другие лидеры прошлого года – Египет, Турция, Вьетнам стали заметно менее интересны киберпреступникам. Одновременно с этим значительно выросло число атак на граждан США, Германии, Великобритании и России.

По нашему мнению, такое изменение в направлении атак является еще одним следствием мирового экономического кризиса. Денег в Сети стало значительно меньше, и начавшийся было рост числа пользователей интернет-банкинга в ряде стран замедлился. Преступникам пришлось переключиться на более «богатые» рынки, где вероятность заработать на заражении пользователей

значительно выше.

Свой вклад в этот процесс внесли и китайские преступники, которые стали меньше атаковать своих же сограждан. О снижении активности игровых троянцев мы уже писали. Вероятно, в ситуации с атаками через Web мы наблюдаем последствия этой же тенденции.

Сетевые атаки

Неотъемлемой частью современной антивирусной программы является файервол. Он позволяет блокировать различные атаки, осуществляемые на компьютер извне не через браузер, а также противодействует попыткам кражи с компьютера пользовательских данных.

В состав Kaspersky Internet Security включен файервол с функцией детектирования входящих пакетов (IDS), многие из которых являются эксплойтами, использующими уязвимости в сетевых службах операционных систем, и способны вызвать заражение непропатченной системы или предоставить злоумышленнику полный доступ к ней.

В 2009 году система IDS, реализованная в KIS2010, отразила 219 899 678 сетевых атак. Аналогичный показатель 2008 года составлял чуть более 30 млн инцидентов.

		Кол-во	%
1	DoS.Generic. SYNFlood	156550484	71,192
2	Intrusion.Win. NETAPI.buffer- overflow.exploit	32605798	14,828
3	Intrusion.Win. MSSQL.worm. Helkern	23263431	10,579
4	Intrusion.Win. DCOM.exploit	3245943	1,476
5	Scan.Generic. UDP	1799685	0,818
6	Intrusion.Win. LSASS.exploit	812775	0,370
7	Intrusion. Generic.TCP. Flags.Bad. Combine.attack	604621	0,275
8	Intrusion.Win. LSASS.ASN1- kill-bill.exploit	555107	0,252

		Кол-во	%
9	DoS.Generic. ICMPFlood	131925	0,060
10	Scan.Generic. TCP	101737	0,046
11	Intrusion.Win. HTTPD.GET. buffer-overflow. exploit	86511	0,039
12	Intrusion.Win. MediaPlayer. ASX.buffer- overflow.exploit	24375	0,011
13	Intrusion.Win. SMB.CVE-2009- 3103.exploit	19378	0,009
14	Intrusion.Win. WINS.heap- overflow.exploit	15200	0,007
15	Intrusion. Generic. OmniWeb.Alert. format-string. exploit	14291	0,006
16	Intrusion.Win. Messenger. exploit	10296	0,005
17	DoS.Win. IGMP.Host- Membership- Query.exploit	8976	0,004
18	Intrusion.Win. PnP.exploit Intrusion.Win. EasyAddress	8783	0,004
19	WebServer. format-string. exploit	6561	0,003
20	DoS.Generic. Land	3505	0,002
			99,986

На первом месте, как и в прошлом году, находится простая и распространен-

ная атака Dos.Generic.SYNFlood, которая при успешном исполнении приводит к отказу в использовании атакуемого компьютера. Такой тип атак сегодня успешно отражается большинством современных систем обнаружения.

На второе место попала более интересная и опасная угроза – NETAPI.bufferoverflow.exploit, которая является реализацией уязвимости MS08-067.

Это та самая уязвимость, которую использовал печально известный червь Kido. Она была обнаружена в конце 2008 года и в аналогичном рейтинге того же года заняла четвертое место. В 2009 году на долю Kido, несомненно, приходится львиная доля из 32 миллионов обнаруженных и заблокированных попыток заражения компьютеров с использованием MS08-067.

Продолжает существовать в Сети и червь Helkern (Slammer). Несмотря на то, что ему исполняется уже 7 лет, он продолжает находиться в лидерах – на него пришлось 23 миллиона заблокированных попыток заражения. Таким же долгожителем является и эксплойт, занявший четвертое место - RPC-DCOM (MS03-026). Эта же уязвимость вызвала глобальную эпидемию червя Lovesan в августе 2003 года.

Локальные заражения

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры не через Web, почту или сетевые порты.

Наши антивирусные решения успешно обнаружили более 100 000 000 (107 370 258) вирусных инцидентов на пользовательских компьютерах, участвующих в Kaspersky Security Network.

Всего в данных инцидентах было зафиксировано 703 700 разных вредоносных и потенциально нежелательных программ.

На долю первых ста из них пришлось 28 597 901 инцидентов, или 27%.

Вредоносные программы из первой двадцатки являются наиболее распространенными угрозами 2009 года.

Место	Детектируемый объект	Количество уникальных компьютеров, на которых был обнаружен объект
1	HEUR:Trojan.Win32.Generic	3050753
2	Net-Worm.Win32.Kido.ih	2924062
3	Virus.Win32.Sality.aa	1407976
4	Net-Worm.Win32.Kido.ir	1176726
5	UDS:DangerousObject.Multi.Generic	620716

Место	Детектируемый объект	Количество уникальных компьютеров, на которых был обнаружен объект
6	Packed.Win32.Black.d	527718
7	Net-Worm.Win32.Kido.iq	518120
8	HEUR:Worm.Win32.Generic	516467
9	Virus.Win32.Virut.ce	488852
10	not-a-virus:AdWare.Win32.Boran.z	466106
11	Virus.Win32.Induc.a	455798
12	HEUR:Trojan-Downloader.Win32.Generic	436229
13	HEUR:Trojan.Win32.StartPage	412245
14	MultiPacked.Multi.Generic	377741
15	Trojan-Downloader.Win32.VB.eql	362685
16	Worm.Win32.FlyStudio.cu	361056
17	Trojan-Dropper.Win32.Flystud.yo	356950
18	Packed.Win32.Black.a	333705
19	Packed.Win32.Klone.bj	320665
20	Trojan.Win32.Chifrax.a	296947

Более чем на трех миллионах компьютеров были заблокированы попытки заражения, которые были успешно обнаружены с помощью эвристических методов. Большинство реализованных таким способом детектов попали в рейтинг: это HEUR:Trojan.Win32.Generic, HEUR:Worm.Win32.Generic, HEUR:Trojan-Downloader.Win32.Generic и HEUR:Trojan.Win32.StartPage.

На деле же, как мы уже говорили, главной эпидемией года стал червь Kido (Conficker), поразивший миллионы компьютеров по всему миру. В двадцатку наиболее распространенных угроз попали сразу три модификации данного червя – Kido.ir, Kido.ih и Kido.iq, и в общей сложности они по количеству скомпрометированных компьютеров опережают лидера - HEUR:Trojan.Win32.Generic более чем на полтора миллиона.

Следующим после Kido идет Sality.aa, который вызвал всемирную эпидемию в прошлом году и лидировал в нашем годовом отчете. Надо отметить, что продержался он недолго – сетевые черви вновь завоевали свои позиции.

Однако помимо Sality в рейтинге присутствуют еще два вируса, один из кото-

рых является классическим файловым, а второй даже не вписывается в существующую классификацию.

Первый – это Virus.Win32.Virut.ce, который, помимо основного функционала – заражения исполняемых файлов, инфицирует веб-сервера, а также распространяется с помощью пиринговых сетей. Эпидемия этого вируса тоже была одним из наиболее заметных событий года.

Второй – Virus.Win32.Induc.a – очень интересный образец творчества создателей вредоносных программ, для своего размножения использующий механизм двухшагового создания исполняемых файлов, реализованный в среде Delphi. Согласно данному механизму, исходный код разрабатываемых приложений сначала компилируется в промежуточные .dcsu-модули, из которых затем собираются исполняемые в Windows файлы. К счастью, этот вирус в настоящее время не несет функциональной нагрузки помимо самого заражения, однако демонстрирует потенциально новый вектор реальных заражений. Следует заметить, что причиной запоздалого обнаружения Induc (зараженные файлы появились в конце 2008 года, а обнаружен он был лишь в августе 2009) является именно отсутствие в нем какого-либо вредоносного функционала помимо размножения.

Благодаря системе мгновенного обнаружения угроз – UDS, работающей в составе Kaspersky Security Network, более 600 000 компьютеров пользователей были защищены в режиме реального времени: новые вредоносные файлы максимально оперативно детектировались как UDS: DangerousObject.Multi.Generic.

Отметим также большое количество вредоносных программ, созданных с помощью скриптового языка FlyStudio. Таких в рейтинге целых 3: Worm.Win32.FlyStudio.cu, Trojan-Dropper.Win32.Flystud.yo и Packed.Win32.Klone.bj. Учитывая, что FlyStudio пользуются в основном китайские злоумышленники, попадание в двадцатку этих программ подтверждает сказанное в первой части отчета: Китай сейчас действительно является одним из ведущих поставщиков вредоносных программ.

Еще одной ярко проявившейся тенденцией в создании вредоносных программ в этом году стала их упаковка и обфускация с помощью специально созданных упаковщиков, что усложняет задачу обнаружения и детектирования даже уже известных образцов. В рейтинг попали несколько представителей подобных упаковщиков, которые принадлежат поведению Packed: это Black.a, Black.d и Klone.bj.

Уязвимости

Уязвимости в программных продуктах являются наиболее опасным видом угроз для компьютеров пользователей. Они могут предоставить злоумышленникам возможность обойти имеющиеся средства защиты и атаковать компьютер.

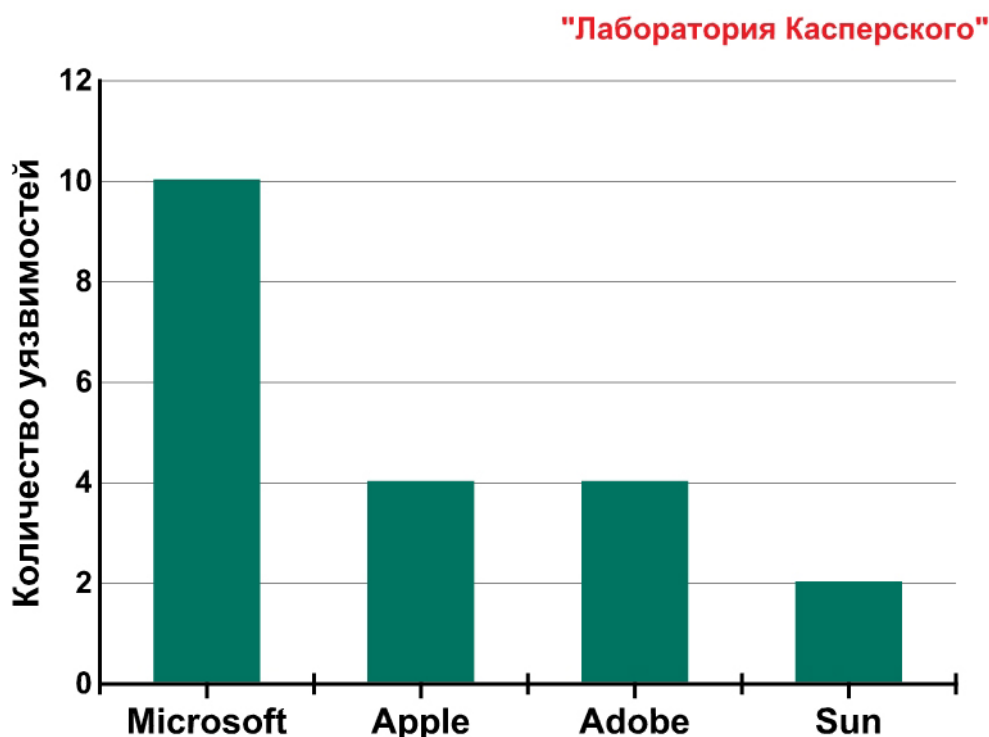
Самая громкая эпидемия 2009 года – червь Kido произошла именно из-за обнаружения очередной критической уязвимости в операционной системе Windows.

Однако, как и год назад, заражение через браузер является наиболее распространенным способом проникновения вредоносных программ в систему. При этом сам браузер может не иметь уязвимостей, но заражение возможно, если уязвимости присутствуют в различных плагинах и приложениях, с которыми браузер взаимодействует.

По итогам работы системы анализа уязвимостей в 2009 году нами было обнаружено 404 различных уязвимости. При этом общее количество уязвимых файлов и приложений на компьютерах пользователей составило 461 828 538.

Мы проанализировали 20 наиболее распространенных уязвимостей. На их долю пришлось 90% (415608137) уязвимых файлов и приложений, обнаруженных на компьютерах пользователей наших антивирусных решений.

Пожалуйста смотрите таблицу на последней странице.



Из пяти наиболее распространенных уязвимостей первые две были обнаружены в 2009 году, вторая и третья – в 2008, а Microsoft XML Core Services Multiple Vulnerabilities, оказавшаяся в таблице на пятом месте, еще в 2007 году.

По числу файлов и приложений, обнаруженных на пользовательских компьютерах, самыми распространенными в 2009 году стали уязвимости в продукте компании Apple – QuickTime 7.x. Более 70% всех уязвимостей обнаруже-

ны именно в этом продукте. При этом следует отметить, что в прошлом году QuickTime также был лидером по числу уязвимостей (более 80%).

Рассмотрим, в продуктах какой компании было обнаружено более всего уязвимостей из первой двадцатки:

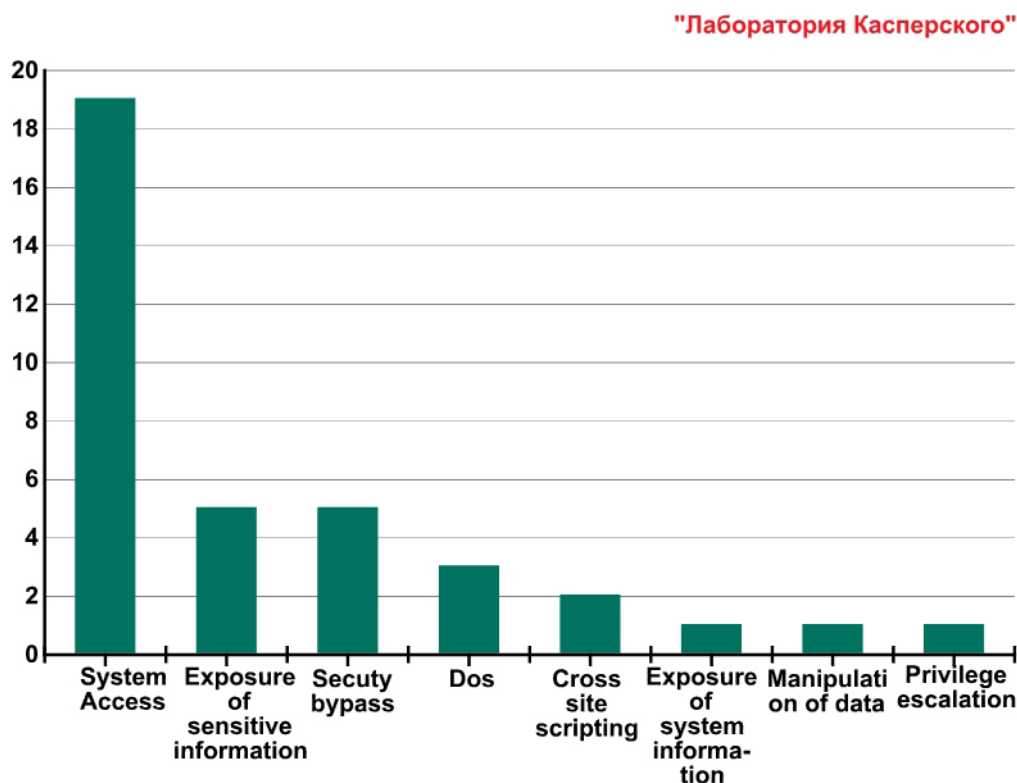
В прошлом году в этом списке находилось 7 компаний, сейчас же их количество сократилось до четырех.

Вновь, как и год назад, лидирует Microsoft с 10 уязвимостями, что, впрочем, не удивительно, так как мы рассматриваем именно ситуацию на платформе Windows. 9 из этих уязвимостей обнаружены в приложениях, входящих в состав Microsoft Office: Word, Excel, Outlook, PowerPoint и т.д.

На Apple пришлось 4 уязвимости – все они обнаружены в QuickTime.

Таким образом можно констатировать, что ситуация полностью аналогична 2008 году – самыми уязвимыми приложениями на современных Windows-системах остаются QuickTime и MS Office.

Впрочем, отставание от них третьей популярной софтверной компании – Adobe, – не столь уж велико. Все четыре уязвимости, записанные на ее счет, принадлежат одному и тому же продукту – Adobe Flash Player. Из четырех уяз-



вимостей две были обнаружены в этом году. И вновь ситуация за год не изменилась к лучшему – скорее только ухудшилась.

Рейтинг наиболее опасных приложений 2009 года выглядит следующим образом:

1. QuickTime
2. Microsoft Office
3. Adobe Flash Player

Если сгруппировать двадцать наиболее распространенных уязвимостей по типам воздействия, то мы получим следующий график:

Все двадцать наиболее часто обнаруживаемых уязвимостей относятся к категории «remote», что подразумевает возможность их использования злоумышленником удаленно, даже если он не имеет локального доступа к компьютеру.

Использование каждой из этих уязвимостей приводит к разным последствиям для атакованной системы. Самым опасным является тип воздействия «system access», позволяющий злоумышленнику получить практически полный доступ к системе.

19 уязвимостей открывают возможности для «system access», 5 способны привести к утечке важной информации.

№	Vulnerability	Число уязвимых файлов и приложений	% от всех уязвимых файлов и приложений	Rating	Impact	Release Date
1	Apple QuickTime Multiple Vulnerabilities	165658505	35,87	Highly Critical	System Access	22.01.09
2	Apple QuickTime Multiple Vulnerabilities	68645338	14,86	Highly Critical	System Access	22.05.09
3	Apple QuickTime Multiple Vulnerabilities	58141113	12,59	Highly Critical	System Access	10.09.08
4	Apple QuickTime Multiple Vulnerabilities	38368954	8,31	Highly Critical	System Access	10.06.08
5	Microsoft XML Core Services Multiple Vulnerabilities	8906277	1,93	Highly Critical	Cross Site Scripting, DoS, System access	09.01.07
6	Adobe Flash Player Multiple Vulnerabilities	7728963	1,67	Highly Critical	Security Bypass, Exposure of sensitive information, Privilege escalation, System access	25.02.09
7	Sun Java JDK / JRE Multiple Vulnerabilities	6783414	1,47	Highly Critical	Security Bypass, DoS, System access	26.03.09
8	Microsoft Outlook "mailto:" URI Handling Vulnerability	6336962	1,37	Highly Critical	System Access	11.03.08
9	Microsoft Excel Multiple Vulnerabilities	6290278	1,36	Highly Critical	System Access	09.06.09

№	Vulnerability	Число уязвимых файлов и приложений	% от всех уязвимых файлов и приложений	Rating	Impact	Release Date
10	35377 Microsoft Office Word Two Vulnerabilities	6088207	1,32	Highly Critical	System Access	09.06.09
11	34572 Microsoft PowerPoint OutlineTextRefAtom Parsing Vulnerability	5704617	1,24	Extremely Critical	System Access	03.04.09
12	31744 Microsoft Office OneNote URI Handling Vulnerability	5652570	1,22	Highly Critical	System Access	09.09.08
13	32270 Adobe Flash Player Multiple Security Issues and Vulnerabilities	5078221	1,10	Moderately critical	Security Bypass, Cross Site Scripting, Manipulation of data, Exposure of sensitive information	16.10.08
14	35948 Adobe Flash Player Multiple Vulnerabilities	5073297	1,10	Highly Critical	Security Bypass, Exposure of sensitive information, System access	23.07.09
15	30285 Microsoft Office Word Multiple Vulnerabilities	4984582	1,08	Highly Critical	System Access	09.12.08
16	31453 Microsoft Office PowerPoint Multiple Vulnerabilities	4203122	0,91	Highly Critical	System Access	12.08.08
17	30150 Microsoft Publisher Object Handler Validation Vulnerability	3965019	0,86	Highly Critical	System Access	13.05.08

№	Vulnerabilty	Число уязвимых файлов и приложений	% от всех уязвимых файлов и приложений	Rating	Impact	Release Date
18	32991 Sun Java JDK / JRE Multiple Vulnerabilities	2980650	0,65	Highly Critical	Security Bypass, Exposure of system information, Exposure of sensitive information, DoS, System access	04.12.08
19	31593 Microsoft Excel Multiple Vulnerabilities	2604816	0,56	Highly Critical	System Access	09.12.08
20	26027 Adobe Player Flash Multiple Vulnerabilities	2413232	0,52	Highly Critical	Exposure of sensitive information, System access	11.07.07
	Top20	415608137	89,99			