УДК 004.056.57

КЛАССИФИКАЦИЯ И СОВРЕМЕННЫЕ УРОВНИ КОМПЬЮТЕРНЫХ УГРОЗ

Бегалин А.Ш. – магистр естественных наук, ст. преподаватель, Костанайский государственный университет им. А.Байтурсынова, г.Костанай.

В данной статье рассматривается классификация современных типов угроз – естественные, искусственные. При этом искусственные угрозы делятся на непреднамеренные и преднамеренные. Источники угроз могут быть как внешними, так и внутренними, приводятся их примеры. Также говорится о том, что бывает источниками компьютерных угроз. Анализируется современный уровень угроз по данным лаборатории Касперского, на основании их отчета, который выходит ежегодно. Приводятся данные о превышении уровня Интернет-атак в 1.7 раза по сравнению с предыдущим годом. В этом анализе угроз приводятся и данные по Республике Казахстан – он один из лидеров заражения через Интернет. Рассматривается также возможный ущерб от атак вредоносных программ - ущерб от попадания в компьютер или корпоративную сеть. Вирус может приводить к ошибкам системы и сети. Бывает что возможен и выход из строя аппаратной части компьютера, например микросхемы BIOS. Подчеркивается необходимость делать копии важных данных.

Ключевые слова: вирус, компьютерные угрозы, Интернет-атаки, эксплойты, заражение, вредоносная программа.

CLASSIFICATION AND CURRENT LEVELS OF COMPUTER THREATS

Begalin A. Sh. - senior teacher of Kostanay state university of a name of A.Baytursynov, master of natural sciences, Kostanay.

In given article classification of the modern types of threats – natural, artificial is considered. Thus artificial threats share on inadvertent and deliberate. Sources of threats can be both exterior, and internal, their examples are resulted. Also it is said that happens sources of computer threats. The modern level of threats according to Kaspersky's laboratory, on the basis of their report which quits annually is analyzed. The data about excess of level of Internet attacks 1.7 times in comparison with previous year is cited. In this analysis of threats the data on Republic Kazakhstan – it one of leaders of infection through the Internet is resulted also. The possible damage from attacks of harmful programs – a damage from hit in the computer or a corporate network is considered also. The virus can lead to system and network errors. Happens that failure of the hardware of the computer, for example chips BIOS is possible also. Necessity to do a copy of the important data is underlined.

Key words: virus, computer threats, cyber attacks, exploits, infection, malware.

КОМПЬЮТЕРЛІК ҚАУПТЕРДІҢ КЛАССИФИКАЦИЯСЫМЕН ҚАЗІРГІ ДЕҢГЕЙЛЕР

Бегалин А.Ш. - Қостанай қ., А. Байтұрсынов атындағы Қостанай мемлекеттік университетінің аға оқытушы, *жаратылыс ғылымдарының магистрі.*

Бұл мақалада қазіргі қауіптің шынайы және жасанды түрлері қарастырылады. Бұл тұрғыда жасанды қауіп жоспарлы, жоспарсыз болып екіге бөлінеді. Қауіптің ішкі және сыртқы жолдары бар және оған мысал келтіріледі. Сонымен қатар бұл мақалада компьютерлік қауіптің болатыны айтылған. Касперлік зертхананың қорытындысы бойынша қауіптің денгейі жыл сайын шығып тұрады. Өткен жылмен салыстыру бойынша Интернет шабуыл денгейінің 1.7 жоғарлауы туралыда сөз қозғалған. Бұл қорытынды да Қазақстан Республикасындағы интернет арқылы жұғатын қауіптер де мысалға келтірілген. Сонымен қатар зиянды бағдарламалар шабуылынан болатын шығындар қарастырылады - компьютерге немесе корпоративтік желідегі шығын. Вирус желідегі қателіктерге апарады. Кейде компьютерлік желіден шығып кететін кездер де болады. Мысал үшін BIOS микросхемасын айта аламыз. Сондықтан қажетті құжаттын көшірмесін жасау керек.

Кілтті сөздер: вирус, комьютерлік қауіп, интернет шабуыл, эксплойттар, қауіпті бағдарламалар.

Классификация угроз

Всё множество потенциально опасных угроз по принципу их возникновения можно разделить на два типа: естественные (объективные) и искусственные (субъективные), в соответствии с рисунком 1.

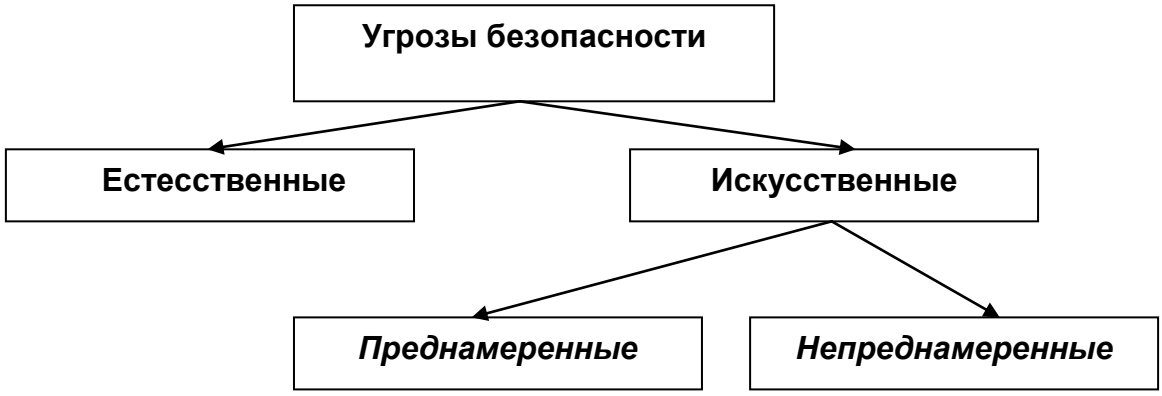

Рисунок 1 - Классификация угроз безопасности

Естественные угрозы - это те угрозы, которые вызваны воздействием на компьютерные системы, а также ее элементы объективными физическими процессами или стихийными природными явлениями, независящих от человека.

Искусственные угрозы - это угрозы компьютерным системам, вызванные деятельностью человека. Из них можно выделить следующие:

– непреднамеренные (случайные, неумышленные) угрозы, которые вызваны ошибками в проектировании вычислительных систем, ошибками в программном обеспечении и действиях персонала и т.д.;

– преднамеренные (умышленные) угрозы, связанные с корыстными намерениями людей (злоумышленников).

Источники угроз для компьютерных систем могут быть как внешними, так и внутренними [5].

С проблемой вредоносных программ мы сталкиваемся практически каждый день. Сейчас количество вредоносных программ измеряется уже миллионами. Есть даже такие вирусы, которые шифруют жесткий диск – от них спастись можно только с помощью резервных копий [6].

Работа на незащищенных компьютерах чревата не только потенциальной угрозой хищения конфиденциальной информации — в этом случае появляется угроза выведения из строя, как отдельных компьютеров, так и целых корпоративных сетей [7].

Современный уровень компьютерных угроз

По данным исследования лаборатории Касперского, количество атак через веб-браузер за 2012 год увеличилось с 946 393 693 до 1 595 587 670. Число отраженных в 2012 году интернет-атак превышает аналогичный показатель 2011 года в 1,7 раза. Основной способ атаки - через эксплойты - дает злоумышленникам практически гарантированную возможность заражения компьютеров, если на них не установлена защита и имеется хотя бы одно популярное и уязвимое приложение [8].

В течение года лабораторией Касперского зарегистрировано как массовые атаки с использованием наборов эксплойтов, так и целевые атаки, в которых использовались Java-эксплойты, нацеленные как на PC, так и на Mac, в соответствии с рисунком 2.

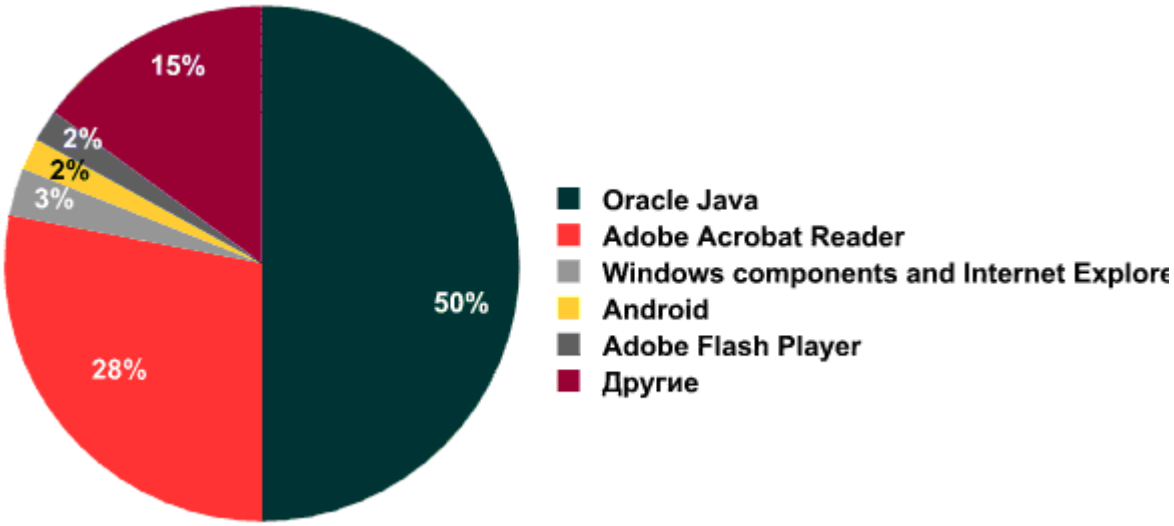

Рисунок 2 - Приложения, уязвимости в которых использовали эксплойты (по данным Лаборатории Касперского)

По данным лаборатории Касперского на третьем месте расположились программы, использующие уязвимости в компонентах Windows и Internet Explorer. Атаки на компьютеры пользователей Windows продолжаются: проникновения в систему, происходят в основном не через компоненты Windows, а через установленные приложения других производителей [8].

Из всех вредоносных программ, участвовавших в интернет-атаках на компьютеры пользователей, можно выделить 20 наиболее активных, в таблице 1 приведено первые пять. На них пришлось 94% всех атак в интернете (См. таблицу 1).

Таблица 1 - Вредоносные программы, участвовавшие в интернет-атаках

Место	Название	Количество атак	% от всех атак
1	Malicious URL	1 393 829 795	87,36%
2	Trojan.Script.Iframer	58 279 262	3,65%
3	Trojan.Script.Generic	38 948 140	2,44%
4	Trojan.Win32.Generic	5 670 627	0,36%
5	Trojan-Downloader.Script.Generic	4 695 210	0,29%

Среди серверов, на которых был размещен вредоносный код, лидируют США и Россия. Наша Республика Казахстан в этот список не входит.

Очень важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают те объекты, которые проникли на компьютеры не через Интернет и почту, а локально, то есть, например, с «флешек», дисков или по локальной сети. (См. таблицу 2) [7].

Таблица 2 - Статистика локальных заражений

Место	Детектируемый объект	Кол-во уникальных пользователей	%
1	Trojan.Win32.Generic	9 761 684	22,1%
2	DangerousObject.Multi.Generic	9 640 618	21,9%
3	Trojan.Win32.AutoRun.gen	5 969 543	13,5%
4	Trojan.Win32.Starter.yy	3 860 982	8,8%
5	Virus.Win32.Virut.ce	3 017 527	6,8%

Наибольший интерес представляет риск заражения через интернет, который является основным источником вредоносных объектов для пользователей большинства стран мира (См. таблицу 3).

Таблица 3 - Заражения через интернет

Место	Страна	% уникальных пользователей
1	Россия	58,6%
2	Таджикистан	58,5%
3	Азербайджан	57,1%
4	Армения	55,7%
5	Казахстан	55,5%
6	Белоруссия	51,8%
7	Бангладеш	51,7%
8	Шри-Ланка	51,5%
9	Индия	51,1%
10	Туркменистан	51,0%

Как видим, Казахстан находится в пятерке лидеров с показателем 55,5%.

В среднем по миру уровень опасности интернета второй год подряд увеличивается и по итогам 2012 года составил 34,7% — на 2,4% больше, чем в прошлом году. Каждый третий пользователь интернета в мире хотя бы раз в год подвергается компьютерной атаке [8].

Ущерб от атак вредоносных программ

Ущерб от попадания вредоносной программы в компьютер или корпоративную сеть может быть разным: от небольшого увеличения сетевого трафика до отказа системы или сети, а также потери важной информации. Но все-таки ущерб от вируса зависти от цели вируса и часто бывает, что работа вируса в системе незаметна для пользователя.

Замедление работы компьютеров или их отказ может быть как случайным, так и преднамеренным. Уничтожение вирусом важных файлов системы может привести к зависаниям, торможениям и неработоспособности системы.

Часто бывает, что вирус (ошибки в его коде или в самой логике работы вируса) приводит к фатальным ошибкам системы и даже сети. Это может происходить по той причине, что после разработки вируса они не проходят тестирование, как коммерческие продукты, а также может быть несовместимость с железом или программами на компьютере. Вследствие этого происходят различные нежеланные ошибки, помимо цели самого вируса. Выход из строя аппаратной части компьютера случается все-таки крайне редко, но бывает. Примером тому вирус Чернобыль, который стирал информацию в микросхеме BIOS на основе Flash-памяти [9].

Если атака осуществляется для того чтобы уничтожить или украсть информацию, то ее стоимость равна стоимости данной информации. Конечно, если взломан домашний компьютер, где важного ничего нет, то цена минимальна, а если украдена или уничтожена важная информация, которая хранилась в единственном экземпляре или секретная, то последствия после успеха такой атаки тяжелые. В этом случае необходимо делать копии важных данных на других носителях, например на флешке и т.д.

ЛИТЕРАТУРА:

1. Безмалый В.Ф. Организация защиты информации центров авторизации карт платежных систем VISA, EUROPAY / В. Безмалый, В. Главатый. - М., 2009. – Режим доступа: http://www.oszone.net

2. Елманова Н. Что угрожает современному пользователю / Н. Елманова // Журнал Компьютер Пресс №5. - М., 2009. – 125 с.

3. Безмалый В.Ф. Угрозы домашнему компьютеру / В. Безмалый // Журнал Компьютер Пресс №11. - М., 2008. – 124 с.

4. Масленников Д. Kaspersky Security Bulletin 2012. Основная статистика за 2012 год / Д. Масленников., Ю. Наместников. - М., 2013. – Режим доступа: http://www.securelist.com

5. Никитина Т. Ущерб от атак вредоносных программ. – Режим доступа: http://www.securelist.com.

References:

1. Bezmalyiy V.F. Organizatsiya zaschityi informatsii tsentrov avtorizatsii kart platezhnyih sistem VISA, EUROPAY / V. Bezmalyiy, V. Glavatyiy. - M., 2009. – Rezhim dostupa: http://www.oszone.net

2. Elmanova N. Chto ugrozhaet sovremennomu polzovatelyu / N. Elmanova // Zhurnal Kompyuter Press #5. - M., 2009. – 125 s.

3. Bezmalyiy V.F. Ugrozyi domashnemu kompyuteru / V. Bezmalyiy // Zhurnal Kompyuter Press #11. - M., 2008. – 124 s.

4. Maslennikov D. Kaspersky Security Bulletin 2012. Osnovnaya statistika za 2012 god / D. Maslennikov., Yu. Namestnikov. - M., 2013. – Rezhim dostupa: http://www.securelist.com

5. Nikitina T. Uscherb ot atak vredonosnyih programm. – Rezhim dostupa: http://www.securelist.com.

Сведения об авторах

Бегалин Алибек Шакиржанович – старший преподаватель кафедры Информатики и математики Костанайского государственного университета им. А. Байтурсынова, магистр естественных наук, г.Костанай, ул. Пушкина 135-83, тел. 87773010081, e-mail: alikbeg@mail.ru.

Begalin Alibek Shakirzhanovich - senior lecturer in Computer Science and Mathematics Kostanai State University. A.Baitursynov, M.Sc., Kostanai str. Pushkin 135-83, tel. 87773010081, e-mail: alikbeg@mail.ru.

Бегалин Алибек Шакиржанович - А. Байтұрсынов атындағы Қостанай мемлекеттік университетінің информатика және математика кафедрасының аға оқытушы, жаратылыс ғылымдарының магистрі, Қостанай қ, Пушкин көш., 135-83, тел. 87773010081, e-mail: alikbeg@mail.ru.