1. Computer crime is not only exploding in volume but is mutating faster than it can be contained. Some 2.5 million new types of malicious programme have been launched in the past two months alone - more than in the entire last 15 years, according to the latest data from the security firm Trend Micro. The UK now has around 1.25 million "infected" computers. And the average number of PCs across the world sending out spam emails every month shot up to 10 million last year, more than double the 4.2 million in 2006, which was double the 2.1 million in 2005.
2. Cyber crime has become a multi-billion-pound, international criminal industry including unsolicited email "phishing" campaigns to con people out of financial details and passwords.
3. In the age-old contest of good guys against bad guys, each side inspires the other to ever greater levels of sophistication. And as viruses evolve, taking root on everything from digital cameras to USB memory sticks, simply securing a corporate infrastructure may no longer be enough.
4. A key tool for the cyber-criminal is the botnet - a large number of computers that are recruited by a virus and can then be controlled from one place, often without their owner's knowledge. Botnets can include tens of thousands of individual PCs, and have a lot of different types of uses, including mass spamming, propagating yet more viruses, and crashing websites by bombarding them with visitors.
5. The current estimate is that there are 175 million infected computers live on the internet today. And cyber crime is worth billions of dollars. But scams are so diverse, and the techniques are evolving so quickly, that it is almost impossible to estimate the true scale of the problem.
6. In value terms, the biggest scam at the moment is "click fraud", where certain websites that are being paid by advertisers on a per-click basis use botnets to bombard the advertiser's site with apparent interest.

Second is good, old-fashioned, fraud - using creditcard details, online accounts or electronic transfers - based on information stolen either from individuals' computers or from insecure company databases.

Third is extortion - often against gambling sites just before major sporting events - where botnets are

used to prove the site can be knocked down unless payment is received.

7. The criminals' techniques are continually developing. This month, for example, saw the first botnet involving both humans and machines. To bypass security measures in signing up free email accounts, a criminal group set up a high-tech sweatshop in India to process the part of the application that cannot be done automatically.

Киберпреступность остается на шаг впереди

То, что начиналось как деятельность хакеров-гиков, превратилось в международную криминальную индустрию с многомиллиардным оборотом.

Адаптировано по материалам The Independent, 22 марта 2008 г.

1. Компьютерная преступность не только стремительно растет в размерах, но и мутирует быстрее, чем ее можно сдерживать.

Только за последние два месяца было запущено около 2,5 миллионов новых типов вредоносных программ - больше, чем за все последние 15 лет, согласно последним данным охранной фирмы Trend Micro. В настоящее время в Великобритании насчитывается около 1,25 миллиона "зараженных" компьютеров. И среднее количество компьютеров по всему миру, ежемесячно рассылающих спам-письма, в прошлом году выросло до 10 миллионов , что более чем вдвое превышает 4,2 миллиона в 2006 году, что вдвое больше 2,1 миллиона в 2005 году.

2. Киберпреступность превратилась в международную криминальную индустрию с многомиллиардным оборотом, включая кампании "фишинга" по электронной почте с целью выманивания у людей финансовых данных и паролей.

3. В извечном состязании хороших парней с плохими каждая сторона вдохновляет другую на все больший уровень изощренности. И по мере развития вирусы внедряются во все - от цифровых камер до USB-накопителей однако простой защиты корпоративной инфраструктуры может оказаться уже недостаточно.

4. Ключевым инструментом киберпреступника является ботнет - большое

количество компьютеров, которые завербовываются вирусом и затем могут контролироваться из одного места, часто без ведома их владельца. Ботнеты могут включать в себя десятки тысяч отдельных компьютеров и использоваться для множества различных целей, включая массовую рассылку спама, распространение еще большего количества вирусов и сбой веб -сайтов из-за бомбардировки их посетителями.

5. По текущим оценкам, сегодня в Интернете насчитывается 175 миллионов зараженных компьютеров. И киберпреступность обходится в миллиарды долларов. Но мошенничества настолько разнообразны, а методы развиваются так быстро, что оценить истинный масштаб проблемы практически невозможно.

6. В стоимостном выражении самой крупной аферой на данный момент является "мошенничество с кликами", когда определенные веб-сайты, которым рекламодатели платят за клик, используют ботнеты для бомбардировки сайта рекламодателя с явным интересом.

Второе - это хорошее, старомодное мошенничество с использованием данных кредитной карты, онлайн-счетов или электронных переводов, основанное на информации, украденной либо у частных лиц' компьютерах или из небезопасных баз данных компании.

В-третьих, это вымогательство - часто против сайтов азартных игр непосредственно перед крупными спортивными мероприятиями, - когда используются ботнеты, чтобы доказать, что сайт может быть заблокирован, если не будет получен платеж.

7. Методы преступников постоянно совершенствуются.

Например, в этом месяце был создан первый ботнет , в котором участвовали как люди, так и машины. Чтобы обойти меры безопасности при регистрации бесплатных учетных записей электронной почты, преступная группа создала в Индии высокотехнологичный потогонный цех для обработки той части приложения, которая не может быть выполнена автоматически.

Here are some types of cybercrime:

Fraud using e-mail and the Internet
Digital identity theft (theft and use of personal data)
Theft of payment card data and other financial information
Theft and resale of corporate data

Cyberschantage (extortion of money under threat of attack)

Attacks using ransomware (one of the varieties of cyber-sabotage)

Cryptojacking (mining cryptocurrencies using other people's resources)

Cyber Espionage (obtaining unauthorized access to government or corporate data)

Disruption of systems in order to compromise the network

Copyright infringement

Illegal gambling

Online trading of prohibited goods

Cybercrime always implies at least one of the following:

Criminal activity for the purpose of attacking computers using viruses or other malware.

Using computers to commit other crimes.

Cybercriminals, whose goal is to attack computers, can infect them with malware in order to damage or completely disable them, as well as to delete or steal data. Cybercriminals may also target a DoS attack (a denial of service attack), due to which users or customers of the company will not be able to use the website, computer network or software services.

Вот некоторые разновидности киберпреступлений:

Мошенничество с использованием электронной почты и интернета

Кража цифровой личности (хищение и использование личных данных)

Кража данных платежных карт и другой финансовой информации

Хищение и перепродажа корпоративных данных

Кибершантаж (вымогательство денег под угрозой атаки)

Атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа)

Криптоджекинг (майнинг криптовалют с использованием чужих ресурсов)

Кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным)

Нарушение работы систем с целью компрометации сети

Нарушение авторских прав

Незаконное проведение азартных игр

Онлайн-торговля запрещенными товарами

Киберпреступление всегда подразумевает хотя бы одно из указанного:

Преступную деятельность с целью атаки на компьютеры с использованием вирусов или другого вредоносного ПО.

Использование компьютеров для совершения других преступлений.

Киберпреступники, целью которых является атака на компьютеры, могут заражать их вредоносными программами, чтобы повредить или полностью вывести из строя, а также чтобы удалить или похитить данные. Также целью киберпреступников может быть DoS-атака (атака типа «отказ в

обслуживании»), из-за которой пользователи или клиенты компании не смогут пользоваться веб-сайтом, компьютерной сетью или программными сервисами.

Julian Assange started hacking at the age of 16. For this activity, he used the nickname Mendax. In just four years, Assange managed to hack the networks of many corporations, government organizations and educational institutions, including NASA, Lockheed Martin, Stanford University and the Pentagon.

In 2006, he created WikiLeaks, a platform that publishes classified information obtained from anonymous sources or as a result of leaks. In 2010, the US government opened a case against Assange on charges of espionage.

Since 2012, Assange has been living in Ecuador, which granted him political asylum, but in April 2019, the country's authorities deprived him of political asylum and Assange was arrested. He is currently in a British prison.

2. Who exactly is a hacker named Guccifer 2.0 (Guccifer 2.0), it is not known for certain. It may be one person, or it may be a group of people. During the 2016 US presidential election, he hacked the network of the National Committee of the Democratic Party of the USA, after which hundreds of secret documents appeared on WikiLeaks and other similar resources. Some believe that the hacker Guccifer 2.0 who carried out the cyberattack is just an attempt by the Russian special services to divert attention from their participation in the hacking. However, after the conducted research, it was proved that Gucifer is not a Russian at all, but a Romanian.

Thus, Guccifer is the name of a Romanian hacker who hacked the website of the American government and many other political organizations.

After the presidential election, Guccifer disappeared, reappearing in January 2017 to prove that he (they) had nothing to do with the Russian intelligence services.

To date, Anonymous is perhaps the most famous hacker, who, paradoxically, is still unknown. Any hacker can act on behalf of Anonymous – in fact, this is a group that does not have any hierarchy or membership.

Since 2003, Anonymous has attacked many organizations and systems, such as PayPal, Amazon, Westboro Baptist Church, Sony, deep Internet sites, the Church of Scientology, as well as the governments of India, Australia, Syria, the United States and many other countries. At the same time, Anonymus is still active.

Джулиан Ассанж начал заниматься хакерскими атаками с 16 лет. Для этой деятельности он использовал ник Мендакс (Mendax). Всего за четыре года Ассанжу удалось взломать сети множества корпораций, правительственных организаций и образовательных учреждений, включая НАСА, Lockheed Martin, Стэндфордский университет и Пентагон.

В 2006 г. он создал WikiLeaks – платформу, публикующую секретную информацию, полученную из анонимных источников или в результате утечки.

В 2010 году Правительство США возбудило против Ассанжа дело по обвинению в шпионаже.

С 2012 года Ассанж проживал в предоставившем ему политическое убежище Эквадоре, однако в апреле 2019 года власти страны лишили его политического убежища и Ассанж был арестован. В настоящее время он находится в британской тюрьме.

2. Кем именно является хакер по имени Гуччифер 2.0 (Guccifer 2.0), доподлинно неизвестно. Возможно, это один человек, а может быть, группа людей. Во время президентских выборов в США 2016 года им была взломана сеть Национального комитета Демократической партии США, после чего на WikiLeaks и других подобных ресурсах появились сотни секретных документов. Некоторые считают, что осуществивший кибератаку хакер Гуччифер 2.0 – это всего лишь попытка российских спецслужб отвлечь внимание от их участия во взломе. Однако после проведенных исследований было доказано, что Гучифер – вовсе не россиянин, а румын.

Таким образом, Гуччифер – это имя румынского хакера, взломавшего сайт американского правительства и множества других политических организаций.

После президентских выборов Гуччифер исчез, появившись снова в январе 2017 г., чтобы доказать, что он (они) не имеют ничего общего с российскими разведслужбами.

На сегодняшний день Анонимус является, пожалуй, самым известным хакером, который, как ни парадоксально это звучит — до сих пор неизвестен. Действовать от имени Анонимуса может любой хакер – по сути, это группа, не имеющая какой-либо иерархии или членства.

Начиная с 2003 года Анонимус атаковал множество организаций и систем, таких как PayPal, Amazon, Баптистская церковь Вестборо, компания Sony, сайты глубинного интернета, Церковь саентологии, а также правительства Индии, Австралии, Сирии, Соединенных Штатов и множества других стран. При этом Анонимус до сих пор активен.

Theft of the source code of S.T.A.L.K.E.R. 2. Hackers hacked the video game developer company GSC Game World. Criminals were able to access 30 GB of information on the video game S.T.A.L.K.E.R. 2. The attackers' demand was to return the Russian voice acting to the game, otherwise they threatened to publish the archive. GSC Game reported that the employee's PC was hacked.

Leakage of customer data from Ferrari. In March, cybercriminals hacked into the database of personal data of Ferrari customers. The motive was very simple – to get a ransom. The company made a newsletter for customers, in which it announced

that it would not make a deal with hackers. The attackers gained access only to personal information not directly related to finance – they could not find out the card numbers and which specific cars the customers bought

Phishing attack on Reddit. The attackers managed to deceive an employee of the company through a fake website under the guise of one of the corporate ones. They stole his data and tokens for two-factor authorization. The attackers gained access to corporate systems, stole internal documents and sources.

Кража исходников S.T.A.L.K.E.R. 2. Хакеры взломали компанию-разработчика видеоигр GSC Game World. Преступники смогли получить доступ к 30 ГБ информации по видеоигре S.T.A.L.K.E.R. 2. Требованием злоумышленников был возврат русской озвучки игру, иначе они угрожали опубликовать архив. В GSC Game сообщили, что взломали ПК сотрудника.

Утечка клиентских данных из Ferrari. В марте киберпреступники взломали базу персональных данных клиентов Ferrari. Мотив был очень простым – получить выкуп. Компания сделала рассылку для клиентов, в которой сообщила о том, что на сделку с хакерами не пойдет. Злоумышленники получили доступ лишь к личной информации, не касающейся напрямую финансов – узнать номера карт и какие конкретно машины покупали клиенты они не смогли

Фишинговая атака на Reddit. Злоумышленникам через подставной сайт под видом одного из корпоративных, удалось обмануть сотрудника компании. Они украли его данные и токены для двухфакторной авторизации. Злоумышленники получили доступ к корпоративным системам, стянули внутренние документы и исходники.

Regular software and operating system updates
Using antivirus programs and updating them regularly
Using strong passwords
The habit of not following links in spam emails and on untrusted websites
Caution when transferring personal information
Communication via official channels
Attentiveness when visiting websites

Регулярное обновление ПО и операционной системы
Использование антивирусных программ и их регулярное обновление
Использование надежных паролей
Привычка не переходить по ссылкам в спам-письмах и на недоверенных веб-сайтах
Осторожность при передаче личной информации
Общение по официальным каналам
Внимательность при посещении веб-сайтов