Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

Практическая работа №6
для слушателей курса повышения квалификации «Основы компьютерной криминалистики и методики реагирования на инциденты ИБ»

Брянск
БГТУ
2022

Задание 1

Приведите два примера инцидентов ИБ, вызванные заражениями вирусами или червями, а также опишите результат инцидента.

Например:

№,п/п	Описание инцидента	Наименование вируса, ботнета	Описание результата инцидента
1	Атака на департамент полиции Вашингтона	Программа-вымогатель	Группировка Babuk опубликовала в даркнете тысячи конфиденциальных документов столичного департамента полиции. Были обнаружены сотни личных дел полицейских, данные об информаторах и разведывательные отчеты, которые включают информацию из других агентств, включая ФБР и Секретную службу. Ссылка на источник: https://habr.com/ru/company/pt/blog/598845/
2	В результате кибератаки пострадали 15 компаний, являющихся участниками холдинга «Мираторг».	вредоносное ПО Win32:Bitlocker/l!rsm	https://infobezopasnost.ru/blog/news/hakery-atakovali-miratorg/ хакеры использовали вредоносное ПО Win32:Bitlocker/l!rsm, замаскированное под системный файл. Эксперты отметили, что шифровальщик пользуется ошибками в ОС от Microsoft. Вредонос поражает все файлы на заражённых устройствах, делая их недоступными для прочтения и редактирования. Чтобы получить доступ к материалам, необходимо знать код, при помощи которого их скрыл вредонос.

3	Компания кибербезопасности Qrator Labs зафиксировала ботнет из рекордных 160 тысяч устройств, который стал причиной DDoS-атаки компаний в сфере ритейла в конце 2021 года. Целью атаки был сбор данных.	Meris и другие без названия	https://habr.com/ru/news/t/648577/ Во второй половине года наблюдался рост числа развернутых ботнетов (в том числе Meris), а также рекордные DDoS-атаки с использованием HTTP-запросов и атаки на сетевом уровне. В конце 2021 года эксперты предупредили, что 300 тысяч роутеров латвийской компании MikroTik уязвимы для удаленных атак.

Задание 2

Приведите два примера крупных DoS или DDoS атак в России и опишите результат после завершения инцидента.

№,п/п	**Описание атаки**	**Наименование атаки**	**Описание результата атаки**
1	9 сентября 2021 года «Яндекс» раскрыл детали DDoS-атаки, которую компания назвала «крупнейшей в истории».	Кибернападение осуществлено с использованием нового ботнета Mēris	Мощность DDoS-атаки составила почти 22 млн RPS (количество запросов в секунду), что является рекордным значением — по крайней мере, о более крупных кибератаках неизвестно. В результате атака не повлияла на работу сервисов, и данные пользователей не пострадали. Специалисты Яндекса справились с инцидентом. Ссылка на источник: https://xakep.ru/2021/09/09/meris/
2	в 2022 году самыми уязвимыми сегментами станут финансовый, медицинский и телекоммуникацио	В 2022 году увеличилось не только количество атак, но и их длительность – если в 2021	https://infobezopasnost.ru/blog/news/za-god-chislo-ddos-atak-napravlennyh-na-rossijskie-kompanii-vyroslo-v-8-raz/ Эксперты «Лаборатории Касперского» сообщили, что в марте 2022 года хакеры атаковали российский рынок в 8 раз чаще, чем за аналогичный период в прошлом году.

	нный сектора, а также сфера ритейла. Мощность атак, по мнению Хантимирова, вырастет до 2,5-3 Тбит/с. Эксперты сообщают, что в марте 2022 число атак на компании, развивающиеся в сфере финансов, выросло в 2 раза, составив 35% от общего количества киберпреступлений. Число нападений на СМИ выросло в 10 раз, достигнув отметки в 32%.	средняя продолжительность DDoS-нападения составляла 12 минут, то сейчас атаки длятся несколько суток. На данный момент рекордный показатель составляет 145 часов непрерывной атаки.	
3	Официальный новостной канал ОАО «Российские железные дороги» в Telegram сообщил, что в работе веб-сайта компании могут наблюдаться сбои		https://infobezopasnost.ru/blog/news/sajt-kompanii-rzhd-podvergsya-ddos-atake/

	из-за регулярных DDoS-атак.		

Задание 3

Приведите два примера инцидентов ИБ, вызванные Загрузкой ПО, а также опишите результат после завершения инцидента.

№, п/п	Описание инцидента	Наименование атаки	Описание результата инцидента
1	Киберпреступная группировка ShadowHammer взломала утилиту ASUS Live Update для доставки обновлений BIOS, UEFI и ПО на лэптопы и стационарные компьютеры ASUS, внедрила в нее бэкдор и распространяла через официальные каналы	ПО с вирусом	По оценкам экспертов, общее число заражений достигло миллиона пользователей. Ссылка на источник: https://habr.com/ru/company/pt/blog/492778/
2	Когда получатель подключал USB-накопитель к своему компьютеру, устройство выполняло атаку BadUSB. USB-накопитель регистрировал себя как клавиатуру и отправлял на ПК пользователя серию предварительно настроенных автоматических	Системные драйверы USB с вирусом	«С августа 2021 года ФБР получило сообщения о нескольких посылках, содержащих эти USB-устройства, которые были отправлены американским предприятиям в сфере транспорта, страхования и обороны. Посылки были отправлены через почтовую службу США и United Parcel Service», — говорится в уведомлении ФБР. Подробнее: https://www.securitylab.ru/news/528370.php

	нажатий клавиш. Нажатия клавиш запускали PowerShell-команды, которые загружали и устанавливали различные виды вредоносных программ. Таким образом киберпреступники получали административный доступ, а затем перемещались на другие локальные системы. Участники FIN7 затем использовали различные инструменты, в том числе Metasploit, Cobalt Strike, PowerShell-скрипты, Carbanak, GRIFFON, DICELOADER, TIRION, и запускали вымогательское ПО BlackMatter и REvil в скомпрометированной сети. Подробнее: https://www.securitylab.ru/news/528370.php		
3	Google пришлось удалить из своего магазина приложений	Шпионский патч в SDK и загружаемых приложениях	https://smotrim.ru/article/2701265 Шпионская закладка собирала логи о местоположении устройства, телефонные номера, адреса

	целый ряд программ, в которых нашли шпионскую "закладку". По данным СМИ, разработчик вредоносного ПО является подрядчиком американской разведки.		электронной почты, а также сведения о других гаджетах, находящихся поблизости. Кроме того, она имела доступ к буферу обмена и попадающим в него паролям. У закладки была и функция доступа к файлам, включая изображения, видео и документы, пересылаемые через WhatsApp.

Задание 4

Приведите два примера инцидентов ИБ, вызванные обнаружением уязвимости в организации, а также опишите результат после завершения инцидента.

№,п/п	**Описание инцидента**	**Наименование атаки**	**Описание результата инцидента**
1	Уязвимость в IIS, Microsoft Security Bulletin MS01-033	В последние годы было написано множество сетевых червей, пользующихся данной уязвимостью, но одним из наиболее известных является CodeRed	CodeRed был впервые обнаружен 17 июля 2001 года, и, по некоторым оценкам, заразил около 300 тысяч компьютеров, помешал работе множества предприятий и нанес значительный финансовый ущерб компаниям по всему миру. Хотя Microsoft и выпустила вместе с бюллетенем MS01-033 патч, закрывающий используемую червем уязвимость, некоторые версии CodeRed до сих пор продолжают распространяться. Ссылка на источник: https://encyclopedia.kaspersky.ru/knowledge/vulnerabilities-examples/
2	Хакеры атакуют российские организации через новую уязвимость Microsoft Office	уязвимости в MSHTML, движке браузера Internet Explorer HEUR:Trojan.MSOffice.Agent.gen	https://www.kaspersky.ru/about/press-releases/2021_18-rossijskih-organizacij-atakovany-cherez-ranee-neizvestnuyu-uyazvimost-v-microsoft-office Движок MSHTML — это программный компонент, который используется в различных современных операционных системах, как

		PDM:Exploit.Win32.Generic	пользовательских, так и серверных. Уязвимость, о которой идёт речь, позволяет встроить в документ Microsoft Office специальный объект, содержащий ссылку на вредоносный скрипт. Если пользователь открывает заражённый документ, то таким образом он даёт злоумышленникам возможность совершать вредоносные действия на своём компьютере. Эксплуатируется эта уязвимость традиционным способом — путём фишинговой рассылки с почтовым вложением документа.
3	**Компания «Доктор Веб» сообщает об участившихся атаках на крупные российские организации. Злоумышленники шифруют файлы, но при этом не требуют выкупа и не оставляют свои контакты.**	уязвимости ПО Microsoft Exchange: ProxyLogon (CVE-2021-26855) и ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).	https://news.drweb.ru/show/?i=14463&lng=ru Злоумышленники используют уязвимости ПО Microsoft Exchange: ProxyLogon (CVE-2021-26855) и ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). При этом в одном из случаев эксплуатация уязвимости для установки бэкдора произошла ещё в марте 2021-го. Также известно, что доступ к данным административной учетной записи мошенники получают с помощью дампа памяти процесса lsass.exe, используя утилиту ProcDump. Далее с полученной учетной записью администратора они подключаются к контроллеру домена, откуда начинают атаку, устанавливая на устройства в сети Bitlocker и Jetico BestCrypt Volume Encryption. Эти программы злоумышленники используют для шифрования жестких дисков.