УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

CYBER SECURITY THREATS

УДК 004.424

Камбулов Данил Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Kambulov D. A. kambulovdan@yandex.ru

Аннотация

Угрозы кибербезопасности - это действия, совершаемые лицами с вредоносными намерениями, цель которых - украсть данные, нанести ущерб или нарушить работу компьютерных систем. Общие категории киберугроз включают вредоносное ПО, социальную инженерию, атаки типа «человек посередине» (MitM), отказ в обслуживании (DoS) и атаки с использованием инъекций.

Киберугрозы могут исходить из самых разных источников: от враждебных государств и террористических групп до отдельных хакеров и доверенных лиц, таких как сотрудники или подрядчики, которые злоупотребляют своими привилегиями для совершения злонамеренных действий.

Annotation

Cybersecurity threats are actions carried out by persons with malicious intent, the purpose of which is to steal data, damage or disrupt computer systems. Common categories of cyber threats include malware, social engineering, man-in-the-middle (MitM) attacks, denial of service (DoS), and injection attacks.

Cyber threats can come from a wide variety of sources, from hostile states and terrorist groups to individual hackers and proxies, such as employees or contractors, who abuse their privileges to commit malicious acts.

Ключевые слова: киберугроза, DoS атака, атака, вредоносное программное обеспечение, антивирусное программное обеспечение, угроза, информационная безопасность, ущерб.

Keywords: cyber threat, DoS attack, attack, malicious software, antivirus software, threat, information security, damage.

Общие источники киберугроз, к которым относят несколько распространенных источников для организаций:

- **Национальные государства -** враждебные страны могут запускать кибератаки на местные компании и учреждения с целью помешать коммуникации, вызвать беспорядки и нанести ущерб.
- **Террористические организации - террористы** проводят кибератаки, направленные на разрушение или злоупотребление критически важной инфраструктурой, угрожают национальной безопасности, подрывают экономику и причиняют телесные повреждения гражданам.
- **Преступные группы.** Организованные группы хакеров стремятся взломать компьютерные системы с целью получения экономической выгоды. Эти группы используют фишинг, спам, шпионское и вредоносное ПО для вымогательства, кражи частной информации и онлайн-мошенничества.
- **Хакеры -** отдельные хакеры нацелены на организации, используя различные методы атак. Обычно они мотивированы личной выгодой, местью, финансовой выгодой или политической деятельностью. Хакеры часто разрабатывают новые угрозы, чтобы повысить свои криминальные способности и улучшить свое личное положение в хакерском сообществе.
- **Вредоносные инсайдеры** - сотрудник, который имеет законный доступ к активам компании и злоупотребляет своими привилегиями для кражи информации или повреждения компьютерных систем в целях экономической или личной выгоды. Инсайдеры могут быть сотрудниками, подрядчиками, поставщиками или партнерами целевой организации. Они также могут быть

посторонними, которые взломали привилегированную учетную запись и выдают себя за ее владельца [1,2].

Типы угроз кибербезопасности

Атаки вредоносного ПО

Вредоносное ПО - это ПО, которое включает вирусы, черви, трояны, шпионское ПО и программы-вымогатели, и является наиболее распространенным типом кибератак. Вредоносное ПО проникает в систему, как правило, через ссылку на ненадежном веб-сайте или по электронной почте или через загрузку нежелательного программного обеспечения. Он развертывается в целевой системе, собирает конфиденциальные данные, манипулирует и блокирует доступ к компонентам сети, а также может уничтожить данные или полностью выключить систему [3-5].

Вот некоторые из основных типов атак вредоносных программ:

- **Вирусы** - фрагмент кода внедряется в приложение. Когда приложение запускается, запускается вредоносный код.
- **Черви** - вредоносное ПО, которое использует уязвимости программного обеспечения и бэкдоры для получения доступа к операционной системе. После установки в сети червь может выполнять такие атаки, как распределенный отказ в обслуживании (DDoS).
- **Трояны** - вредоносный код или программное обеспечение, которое выдает себя за невинную программу, скрывающуюся в приложениях, играх или вложениях электронной почты. Ничего не подозревающий пользователь загружает троян, позволяя ему получить контроль над своим устройством.
- **Программа-вымогатель** - пользователю или организации запрещен доступ к их собственным системам или данным с помощью шифрования. Злоумышленник обычно требует уплаты выкупа в обмен на ключ дешифрования для восстановления доступа, но нет гарантии, что уплата выкупа фактически восстановит полный доступ или функциональность.
- **Криптоджекинг** - злоумышленники развертывают программное обеспечение на устройстве жертвы и без их ведома начинают использовать свои

вычислительные ресурсы для генерации криптовалюты. Затронутые системы могут стать медленными, а комплекты криптоджекинга могут повлиять на стабильность системы.

- **Шпионское ПО** - злоумышленник получает доступ к данным ничего не подозревающего пользователя, включая конфиденциальную информацию, такую как пароли и платежные реквизиты. Шпионское ПО может повлиять на настольные браузеры, мобильные телефоны и настольные приложения.
- **Рекламное ПО** - активность пользователя в браузере отслеживается для определения моделей поведения и интересов, что позволяет рекламодателям рассылать пользователю целевую рекламу. Рекламное ПО связано со шпионским ПО, но не требует установки программного обеспечения на устройство пользователя и не обязательно используется в злонамеренных целях, но может использоваться без согласия пользователя и ставить под угрозу его конфиденциальность.
- **Бесфайловое вредоносное** ПО - в операционной системе не установлено **программное** обеспечение. Собственные файлы, такие как WMI и PowerShell, редактируются для включения вредоносных функций. Эту скрытую форму атаки трудно обнаружить (антивирус не может ее идентифицировать), поскольку скомпрометированные файлы распознаются как легитимные.
- **Руткиты -** программное обеспечение внедряется в приложения, прошивки, ядра операционных систем или гипервизоры, обеспечивая удаленный административный доступ к компьютеру. Злоумышленник может запустить операционную систему в скомпрометированной среде, получить полный контроль над компьютером и доставить дополнительное вредоносное ПО [6].

Пользователь должен следовать правилам, которые поддерживаются правоохранительными органами. Как и в случае с ремнями безопасности, требуется длительная и упорная воспитательная работа для того, чтобы пользователи осознали необходимость таких мер.

Литература

1. Сорокин, З. Идем в атаку / З. Сорокин. - М.: ДОСААФ, 2016. - 200 с.

2. Шафрин Ю.А. 1500 основных понятий, терминов и практических советов для пользователей персональным компьютером. – М.: Дрофа, 2001. – 272 с
3. Стайн, Р.Л. Атака мутанта / Р.Л. Стайн. - М.: Росмэн, 2016. - 107 с.
4. Фостер, Дж.С. Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров / Дж.С. Фостер. - М.: ДМК, 2009. - 784 с.
5. Чирилло, Д. Обнаружение хакерских атак / Д. Чирилло. - М.: СПб: Питер, 2010. - 864 с.
6. Фридланд А.Я. Информатика и компьютерные технологии: Основные термины: Толков. Слов.: Более 1000 базовых понятий и терминов. – 3-е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. – М.: ООО «Издательство Астрель», 2003. – 272 с.

Literature

1. Sorokin, Z. We go to the attack / Z. Sorokin. - M .: DOSAAF, 2016 .-- 200 p.
2. Shafrin Yu.A. 1500 basic concepts, terms and practical tips for personal computer users. - M .: Bustard, 2001 .-- 272 p.
3. Stein, R.L. Attack of the mutant / R.L. Stein. - M .: Rosmen, 2016 .-- 107 p.
4. Foster, J.S. Protection against hacking: sockets, exploits, shell-code: identifying vulnerabilities of operating systems and applications to hacker attacks / J.S. Foster. - M .: DMK, 2009 .-- 784 p.
5. Cirillo, D. Detection of hacker attacks / D. Cirillo. - M .: SPb: Peter, 2010 .-- 864 p.
6. Friedland A.Ya. Informatics and computer technology: Basic terms: Interpretations. Words .: More than 1000 basic concepts and terms. - 3rd ed. rev. and additional / A.Ya. Friedland, L.S. Khanamirova, I.A. Friedland. - M .: OOO "Astrel Publishing House", 2003. - 272 p.