DOI: 10.12731/2070-7568-2022-11-4-67-76
УДК 004.9

ВЫЯВЛЕНИЕ ОСНОВНЫХ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ МАЛЫХ И БОЛЬШИХ СЕТЕЙ

А.В. Поначугин, А.В. Усердова, Л.Р. Шехмаметьева

В условиях современности достаточно сложно отслеживать все существующие угрозы сетевой безопасности. В статье рассмотрены основные угрозы безопасности для малых и больших сетей в контексте их характеристики и особенностей выявления.

***Цель** – разбор основных угроз безопасности для малых и больших сетей, а также чем они представлены.*

***Метод или методология проведения работы:** при написании статьи использовался анализ научной литературы в области основных вопросов обеспечения сетевой безопасности, с последующим синтезом полученных данных.*

***Результаты:** сформулированы основные угрозы безопасности для малых и больших сетей.*

***Область применения результатов:** полученные результаты могут быть применены в области информационной безопасности и защиты персональных данных.*

***Ключевые слова:** безопасность; большая сеть; малая сеть; угроза*

IDENTIFICATION OF THE MAIN SECURITY THREATS FOR SMALL AND LARGE NETWORKS

A.V. Ponachugin, A.V. Userdova, L.R. Shekhmametyeva

In modern conditions, it is quite difficult to keep track of all existing threats to network security. The article considers the main security threats for small and large networks in the context of their characteristics and features of detection.

Purpose. *Analytical analyze the main security threats for small and large networks, as well as how they are presented.*

Methodology: *when writing the article, the analysis of scientific literature in the field of the main issues of ensuring network security was used, followed by a synthesis of the data obtained.*

Results: *the main security threats for small and large networks are formulated.*

Practical implications: *the results obtained can be applied in the field of information security and personal data protection.*

Keywords: *security; large network; small network; threat*

При работе в больших и малых сетях, когда большинство повседневных действий автоматизированы и доступны в Интернете, необходимо обеспечить высокий уровень предосторожности. Эта предосторожность актуализируется еще больше после появления критической статистики, посредством которой демонстрируется, что почти треть компьютеров в мире заражены тем или иным типом вредоносного программного обеспечения [1, с. 100]. Проблема исследования заключается в том, что процесс отслеживания многообразных угроз сетевой безопасности является весьма трудоёмким, также проблема обусловливается возникновением новых разновидностей угроз, под которые требуется адаптировать механизмы выявления.

Первая группа представлена ввнутренними угрозами, которые, как отмечает В.Е. Чумаков, имеют место, когда сотрудники, персонал организаций халатно относятся к доступу к сетям. Наряду с халатностью, актуализируются случаи злоупотребления [4, с. 61]. Сами угрозы для сетевой безопасности весьма вариабельны. Речь идёт о:

- компьютерных вирусах и червях;
- атаки, сопровождающихся загрузкой данных;
- фишинговых атаках;
- распределенных атаках;
- вредоносной рекламе;
- шпионском программном обеспечении;
- руткитах;

- атаках на базе высокой пропускной способности.

Далее необходимо рассмотреть представленные выше угрозы более детально (в контексте их сущности и специфики выявления).

Для малых и больших сетей существенную угрозу несут компьютерные вирусы и черви.

Следует подчеркнуть, что для обычных пользователей компьютерные вирусы являются одной из самых распространенных сетевых угроз в области кибербезопасности. Компьютерные вирусы – это части программного обеспечения, предназначенные для распространения с одного компьютера на другой. Они часто отправляются в виде вложений электронной почты либо загружаются с определенных веб-сайтов с намерением заразить компьютер и другие компьютеры в списке контактов – с помощью систем в сети.

Известно, что вирусы рассылают спам, отключают настройки безопасности, повреждают и крадут данные с компьютера, включая личную информацию, такую, как пароли, вплоть до удаления всего на жестком диске.

В свою очередь, компьютерные черви – это фрагменты вредоносных программ, которые быстро распространяются с одного компьютера на другой. Червь распространяется с зараженного компьютера, рассылая себя по всем контактам, действуя в масштабах сети: от малой до большой сети. Передача червей также часто осуществляется путем использования уязвимостей программного обеспечения [5, с. 47].

Атаки с загрузкой данных представляют собой серьёзную угрозу для малых и больших сетей. В ходе выявления угрозы следует принимать во внимание то, что при подобных атаках вредоносные коды загружаются с веб-ресурса через браузер, приложение либо встроенную операционную систему без разрешения или ведома пользователя. Пользователю не нужно ничего нажимать, чтобы активировать загрузку. Простой доступ или просмотр веб-сайта может начать загрузку [3, с. 23].

Фишинговые атаки – это тип угрозы безопасности для малых и больших сетей, в которой используется социальная инженерия с целью получения конфиденциальных данных, таких, как:

- пароли;
- имена пользователей;
- номера кредитных карт [2, с. 161].

Таким атаки часто осуществляются в форме мгновенных сообщений или фишинговых электронных писем. Затем получателя электронной почты обманом заставляют открыть вредоносную ссылку, что приводит к установке вредоносного ПО на компьютер получателя.

Важнейшей угрозой сетевой безопасности являются распределенные атаки типа «отказ в обслуживании» (DDoS). Бывают такие случаи, когда сервер перегружается трафиком и просто «падает», иногда, когда выходит новость. Но чаще всего это происходит с веб-сайтом во время DoS-атаки или отказа в обслуживании — вредоносной перегрузки трафика, которая возникает, когда злоумышленники переполняют веб-сайт трафиком. Когда на веб-сайте слишком много трафика, он не может предоставить посетителям свой контент.

Атака DoS выполняется одной машиной и ее подключением к Интернету путем «затопления» веб-сайта пакетами и невозможности доступа пользователей к содержимому веб-сайта. Атака DDoS похожа на DoS, но более мощная. Она запускается с нескольких компьютеров, и количество задействованных машин может варьироваться от пары до тысяч и более. Поскольку вполне вероятно, что не все эти машины принадлежат злоумышленнику, они скомпрометированы и добавлены в сеть злоумышленника с помощью вредоносного ПО. Эти компьютеры могут быть распределены по всему миру, и сеть скомпрометированных компьютеров называется ботнетом. Поскольку атака исходит одновременно с очень многих разных IP-адресов, жертве гораздо труднее обнаружить DDoS-атаку и защититься от нее.

Вредоносная реклама также является угрозой для сетевой безопасности.

Под «рекламным ПО» следует понимать любое программное обеспечение, предназначенное для отслеживания данных о привычках просмотра и на основе этого показа рекламы и всплывающих

окон. Рекламное ПО собирает данные с согласия пользователя и даже является законным источником дохода для компаний, которые позволяют пользователям бесплатно опробовать свое программное обеспечение, но с показом рекламы во время использования.

Пункт о рекламном ПО часто скрыт в соответствующих документах Пользовательского соглашения, но его можно проверить, внимательно прочитав все, что пользователь принимает при установке программного обеспечения.

Присутствие рекламного ПО на компьютере заметно только по всплывающим окнам, и иногда оно может замедлять работу процессора и скорость интернет-соединения. Когда рекламное ПО загружается без согласия, оно считается вредоносным.

Шпионское ПО как угроза для сетей (малых и больших) работает аналогично рекламному ПО, но устанавливается на компьютер без ведома пользователя. Оно может содержать кейлоггеры, которые записывают личную информацию, включая адреса электронной почты, пароли и даже номера кредитных карт, что делает его опасным из-за высокого риска кражи личных данных [6, с. 160].

Руткиты являются одной из явных угроз безопасности для малых и больших сетей. Это набор программных средств, обеспечивающих удаленное управление и доступ на уровне администрирования через компьютер или компьютерные сети. Получив удаленный доступ, руткит может выполнить ряд вредоносных действий; они оснащены кейлоггерами, «похитителями» паролей и антивирусными блокировщиками. Руткиты устанавливаются, скрываясь в лицензионном программном обеспечении: когда пользователь дает этому программному обеспечению разрешение на внесение изменений в ОС, руткит устанавливается на компьютер и ждет, пока злоумышленник не активирует его. Другие способы распространения руткитов включают фишинговые электронные письма, вредоносные ссылки, файлы и загрузку программного обеспечения с подозрительных веб-сайтов.

С появлением новых технологий и сетей 5G более высокая скорость передачи и большие объемы данных могут быть получены и

загружены быстрее, чем когда-либо. Появляются, в связи с этим, и новые угрозы для безопасности малых и больших сетей. Атаки на основе высокой пропускной способности также более распространены, чем когда-либо, они затрагивают большинство технологий, но особенно сосредоточены на «Интернете вещей» и мобильных устройствах. Природа атак предполагает одновременное заражение нескольких устройств, которые впоследствии будут выполнять различные атакующие функции, в зависимости от их роли в координируемой ботом атаке. Этот тип атаки также использует ИИ для обнаружения новых жертв, смены стратегии атаки, а также для сопоставления и обмена данными с первоначальным злоумышленником.

Подводя итоги, необходимо отметить следующее. Может показаться достаточно трудной задачей отслеживать все существующие угрозы сетевой безопасности, а также новые, которые продолжают появляться. Именно поэтому, наравне с противодействием данным угрозам, определяющую роль играет своевременное их выявление. Авторские рекомендации касаются проведения в последующем более детальных научных исследований, ориентированных на систематизацию механизмов выявления угроз, категоризацию этих механизмов на основе классификации угроз. Практическое направление рекомендаций связывается нами с учётом в научных исследованиях успешного опыта использования данных механизмов (с анализом конкретных примеров) для того, чтобы теоретические положения подтверждались практикой.

Список литературы

1. Лысов Д.А. Классификация угроз информационной безопасности, реализуемых с помощью сетевых технологий / Д.А. Лысов, И.В. Горбачев, Н.О. Мусиенко // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Материалы XII Межрегиональной научно-практической конференции. Брянск, 2020. С. 100-103.
2. Полянская В.А., Ожиганова Ю.В., Кузнецов В.П. Современный вклад цифровой экономики в развитие предприятий промышлен-

ной отрасли посредством повышения профессиональных компетенций сотрудников // Экономическое развитие России: тенденции, перспективы. Сборник статей по материалам VIII Международной студенческой научно-практической конференции. Нижний Новгород, 2022. С. 19-23.

3. Рашевский Р.Б. Методы выявления угроз информационной безопасности посредством анализа сетевых взаимодействий / Р.Б. Рашевский, С.И. Козьминых // Информационная безопасность в банковско-финансовой сфере. М., 2020. С. 159-164.
4. Сартаев Б.С. Вопросы обеспечения сетевой безопасности / Б.С. Сартаев // Интеграция сектора исследований и разработок в глобальную инновационную систему. Сборник материалов Международной научно-практической конференции. Кемерово, 2020. С. 21-24.
5. Трифонов Ю.В., Шестерикова Н.В., Рузанов П.А. Развитие интеллектуальных информационно-коммуникационных технологий в экономических и управленческих системах // Экономика и предпринимательство. 2022. № 1 (138). С. 1401-1404.
6. Чумаков В.Е. Алгоритмы сканирования сети на предмет потенциальных уязвимостей / В.Е. Чумаков // Современные научные исследования: теория, методология, практика. Сборник статей по материалам международной научно-практической конференции. Уфа, 2019. С. 158-162.
7. Чумаков В.Е. Анализ методов по организации безопасности сетевой инфраструктуры // Дневник науки. 2019. № 5 (29). С. 60-62.
8. Шаяхметов О.Х. Процесс управления антивирусной безопасностью в организации // Современное гуманитарное знание о проблемах социального развития. Ставрополь, 2022. С. 47-50.

References

1. Lysov D.A., Gorbachev I.V., Musienko N.O. *Informatsionnaya bezopasnost' i zashchita personal'nykh dannykh. Problemy i puti ikh resheniya. Materialy XII Mezhregional'noy nauchno-prakticheskoy konferentsii* [Information security and protection of personal data. Problems and ways to solve them. Materials of the XII Interregional Scientific and Practical Conference]. Bryansk, 2020, pp. 100-103.

2. Polyanskaya V.A., Ozhiganova Yu.V., Kuznetsov V.P. *Ekonomicheskoe razvitie Rossii: tendentsii, perspektivy. Sbornik statey po materialam VIII Mezhdunarodnoy studencheskoy nauchno-prakticheskoy konferentsii* [Economic development of Russia: trends, prospects. Collection of articles based on materials of the VIII International Student Scientific and Practical Conference]. Nizhniy Novgorod, 2022, pp. 19-23.
3. Rashevskiy R.B., Koz'minykh S.I. *Informatsionnaya bezopasnost' v bankovsko-finansovoy sfere* [Information security in the banking and financial sector]. M., 2020, pp. 159-164.
4. Sartaev B.S. *Integratsiya sektora issledovaniy i razrabotok v global'nuyu innovatsionnuyu sistemu. Sbornik materialov Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Integration of the research and development sector into the global innovation system. Collection of materials of the International scientific-practical conference]. Kemerovo, 2020, pp. 21-24.
5. Trifonov Yu.V., Shesterikova N.V., Ruzanov P.A. *Ekonomika i predprinimatel'stvo*, 2022, no. 1 (138), pp. 1401-1404.
6. Chumakov V.E. Algoritmy skanirovaniya seti na predmet potentsial'nykh uyazvimostey / V.E. Chumakov // Sovremennye nauchnye issledovaniya: teoriya, metodologiya, praktika. Sbornik statey po materialam mezhdunarodnoy nauchno-prakticheskoy konferentsii. Ufa, 2019. S. 158-162.
7. Chumakov V.E. *Dnevnik nauki*, 2019, no. 5 (29), pp. 60-62.
8. Shayakhmetov O.Kh. *Sovremennoe gumanitarnoe znanie o problemakh sotsial'nogo razvitiya* [Modern humanitarian knowledge about the problems of social development]. Stavropol', 2022, pp. 47-50.

ДАННЫЕ ОБ АВТОРАХ

Поначугин Александр Викторович, доцент кафедры «Прикладной информатики и информационных технологий в образовании», кандидат экономических наук
Нижегородский Государственный педагогический университет имени Козьмы Минина

ул. Ульянова, 1, г. Нижний Новгород, Нижегородская область, 603005, Российская Федерация
Ponachygin_AV@mininuniver.ru

Усердова Алина Владимировна, студентка кафедры «Физики, математики и физико-математического образования»
Нижегородский Государственный педагогический университет имени Козьмы Минина
ул. Ульянова, 1, г. Нижний Новгород, Нижегородская область, 603005, Российская Федерация
userdova_alya@mail.ru

Шехмаметьева Лилия Равильевна, студентка кафедры «Физики, математики и физико-математического образования»
Нижегородский Государственный педагогический университет имени Козьмы Минина
ул. Ульянова, 1, г. Нижний Новгород, Нижегородская область, 603005, Российская Федерация
lilija.scheh2015@yandex.ru

DATA ABOUT THE AUTHORS

Aleksandr V. Ponachugin, Associate Professor «Applied Informatics and Information Technologies in Education», Candidate of Economic Sciences
Minin Nizhny Novgorod State Pedagogical University
1, Ulyanov Str., Nizhny Novgorod, Nizhny Novgorod region, 603005, Russian Federation
Ponachygin_AV@mininuniver.ru
SPIN-code: 6288-9230
ORCID: https://orcid.org/0000-0001-5518-5565
ResearcherID: S-9446-2018
Scopus Author ID: 57190758241

Alina V. Userdova, Student of the Department of "Physics, Mathematics and Physics and Mathematics Education"

Minin Nizhny Novgorod State Pedagogical University
1, Ulyanov Str., Nizhny Novgorod, Nizhny Novgorod region, 603005, Russian Federation
userdova_alya@mail.ru

Lilia R. Shekhmametyeva, Student of the Department of "Physics, Mathematics and Physics and Mathematics Education"
Minin Nizhny Novgorod State Pedagogical University
1, Ulyanov Str., Nizhny Novgorod, Nizhny Novgorod region, 603005, Russian Federation
lilija.scheh2015@yandex.ru

Поступила 29.11.2022 Received 29.11.2022
После рецензирования 10.12.2022 Revised 10.12.2022
Принята 20.12.2022 Accepted 20.12.2022