Инженерный вестник Дона, №4 (2019)
ivdon.ru/ru/magazine/archive/n4y2019/5859

Современные угрозы безопасности в сети Интернет и контрмеры (обзор)

А.У. Менциев, Х.С. Чебиева

Чеченский государственный университет, Грозный

Аннотация: За последние десятилетия интернет изменил нашу жизнь и способы ведения наших повседневных дел. Интернет изменил методы общения, а для многих предприятий и организаций изменилась технология работы. В сегодняшней бизнес-среде, если у организации нет какого-либо присутствия в интернете она рискует остаться позади своих конкурентов, так как интернет и технологии продолжают развиваться и развивать нас. В данной работе приведен небольшой обзор литературы по угрозам безопасности в интернете. Типичные угрозы классифицированы и показаны их воздействия. Даны методические рекомендации по их минимизации.
Ключевые слова: компьютерная безопасность, угрозы безопасности, спуфинг, отказ в обслуживании, DoS, DDoS, кибербезопасность.

На сегодняшний день, Интернет не особо безопасное место. Это связано с тем, что Интернет является публичной открытой системой, в которой данные двигаются бесконтрольно и могут быть обнаружены, перехвачены или украдены, если применяются правильные знания и оборудование. Такое положение дел вызывает беспокойство, особенно когда конфиденциальные данные, такие как личная или финансовая информация, постоянно передаются через Интернет. Протоколы, используемые в Интернете, общедоступны для исследования, позволяя киберпреступнику одержать верх, поскольку они могут получить полезные знания о том, как функционирует Интернет [1]. Основной протокол, используемый в Интернете, протокол TCP/IP. На ранних этапах его разработки основной целью протокола было обеспечение надежного и стабильного соединения для связи, а не решение проблем с безопасностью. В этом заключается значительная проблема, заключающаяся в том, что протокол является слишком «доверчивым», а это позволяет киберпреступнику использовать преимущества [2].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Согласно данным исследования компании Fact Monster следует, что около 3,035 миллиарда человек во всем мире имеют доступ к Интернету и, следовательно, с точки зрения безопасности, среди них есть огромное количество потенциальных киберпреступников [3]. При таком большом масштабе, достаточно легко оставаться незаметными и уйти с возможными от наказания за киберпреступления. Нет руководящих органов, пресекающих преступные действия в сети Интернет на глобальном уровне. Также стоит отметить, что существуют большие подпольные интернет-сообщества хакеров и киберпреступников, которые делятся своими знаниями и опытом. Это рисует довольно обреченную картину Интернета и его использования для бизнеса, но с правильными процедурами и качественным оборудованием, можно обеспечить безопасность подконтрольных организации систем.

В данной таблице приведена актуальная сводка обсуждаемых угроз.

Таблица 1: Сводка угроз

Название угрозы	Последствия атаки
Вредоносный код	Потеря файлов или потеря работоспособности системы
Прослушивание интернета	Кража конфиденциальной информации
Спуфинг	Несанкционированный доступ к конфиденциальной информации и реализация операций до обнаружения
Отказ в обслуживании	Потеря обслуживания на сервере, веб-сайте, компьютере
Дефрагментация пакетов	Несанкционированный доступ к системе и информации в ней
Технологическая	Потеря работоспособности компьютера и сбор информации о пользователе
Нетехнологическая	Физическое повреждение оборудования, доступ к системной и конфиденциальной информации

Взлом и киберпреступники

Хакером называют человека, который намеревается получить несанкционированный доступ к компьютерной системе. Другой термин, связанный с преступными действиями с использованием компьютеров -

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

«взломщик». Хакеры и взломщики - это тот контингент, что составляет число киберпреступников в Интернете [4]. У них часто есть ряд различных мотивов для атак, которые они проводят, но атаки почти всегда вызывают значительные сбои или финансовые потери. Некоторые киберпреступники рассматривают свои действия, как вызов системе или даже хобби. Они могут, например, просто попытаться получить доступ к системе, а затем уйти, не нанеся никакого ущерба. Другие же имеют серьезные преступные намерения, такие как мошенничество и кража различных данных организаций [5,6]. Далее в работе более подробно рассмотрены некоторые виды атак, используемые киберпреступниками.

Вредоносный код

Вредоносный код включает в себя ряд угроз, таких как атаки вирусов, червей и троянских коней. Вирус - это программа, которая может прикрепляться к файлам на компьютере, заражать их, а затем копировать себя для заражения других файлов [7]. Он может повлиять на компьютеры, которые подключены к главному компьютеру через сетевой канал, вследствие чего они могут довольно быстро распространяться на другие компьютеры через сеть. Популярным способом распространения вируса является электронная почта. В дополнение к способности к репликации большинство компьютерных вирусов способны наносить повреждение, например, это может быть команда, чтобы удалить все файлы в системе или вызвать другие подобные осложнения [8]. Однако, вирусы не всегда легко обнаружить, поскольку они могут скрыть свое присутствие, используя умные алгоритмы. Существуют полиморфные вирусы, которые используют знания о том, как работает антивирусное программное обеспечение, они способны избежать обнаружения. Это указывает на то, что создатели таких вирусов очень умны, следовательно, мы должны быть чрезвычайно бдительны в решении вопросов компьютерной безопасности. Даже простые примитивные

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

вирусы способны нанести вред системам и повлечь огромные финансовые затраты [9].

Прослушивание интернета

В Интернете данные проходят через множество различных сетевых доменов. Маршрутизаторы используются для соединения этих сетевых доменов вместе и для направления трафика в направлении его адреса назначения [10]. Однако, маршрутизатор может использоваться как сигнал, посредством которого злоумышленник может получить доступ к информации, проходящей через них, с помощью программного обеспечения известного как анализатор. Анализаторы - это программы, которые считывают пакеты данных передаваемые по сети. Они часто используются сетевыми администраторами для тестирования производительности сети, но, к сожалению, они также используются киберпреступниками [11]. При использовании анализаторов данные могут быть украдены или изменены, что вызывает серьезную обеспокоенность, учитывая виды передаваемой информации [12].

Спуфинг

Этот тип атаки использует преимущества доверчивой природы TCP/IP. Спуфинг или подмена - это маскировка под чужим именем, чаще всего надежный источник, для сбора информации или осуществления какого-либо другого преступного действия. Хороший пример этого можно увидеть в «атаке маршрутизации от источника». Когда компьютер желает связаться с другим компьютером для отправки данных, они устанавливают сеанс TCP/IP [13]. Вот что происходит:

- Компьютер А хочет общаться с компьютером Б.
- Компьютер А отправляет сообщение на компьютер Б, сообщая, что хочет связаться, и отправляет «начальный порядковый номер».

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

- Компьютер Б получает этот запрос и затем отправляет обратно число-подтверждение со своей собственной последовательностью.
- Компьютер А подтвердит сообщение компьютера Б, после чего может начаться связь [14].

Однако порядковые номера не генерируются случайным образом, и, следовательно, можно определить используемые порядковые номера. Другой компьютер, компьютер В, используемый киберпреступником, может претендовать на звание компьютера А, вычисляя используемый порядковый номер и используя IP-адрес компьютера А. Компьютер В мог бы затем запросить информацию или доступ к информации от компьютера Б, изображающего из себя доверенный компьютер А. [15] Для успешного выполнения этого типа атаки предлагается выполнить ряд задач:

- Доверенный компьютер А должен быть выведен из строя, как правило, путем использования атаки отказа от обслуживания.
- Атакующий компьютер В должен назначить себе IP-адрес доверенного компьютера А.
- Затем компьютер В должен подключиться к компьютеру Б, обманывая его, полагая, что это доверенный компьютер А. Он делает это с помощью IP-адреса компьютера А и с помощью используемых порядковых номеров. Выработка порядковых номеров - самая сложная часть атаки [16].

Отказ в обслуживании

Основной целью этой атаки, как следует из названия, является отказ в обслуживании. Он включает в себя отправку многочисленных запросов на веб-сайт или сервер, чтобы перегружать систему информацией, которую она не может обработать достаточно быстро [17]. Такая атака может привести к сбою сервера или интернет-сайта и, следовательно, к предотвращению доступа клиентов, что может привести к потере репутации и клиентов [18]. Также может распространяться атака типа «отказ в обслуживании», при

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

которой многие компьютеры (ботнет) используются для отправки бесполезных запросов, что приводит к более быстрой и более серьезной атаке [19].

Рекомендуемые контрмеры

Для реализации качественных контрмер, против рассмотренных видов атак, необходимо использовать различные средства контроля для защиты конфиденциальности, целостности и доступности информационных систем. Общая безопасность контролируемых систем может быть значительно улучшена путем добавления дополнительных мер безопасности, удаления ненужных сервисов, усиления защиты систем, ограничения доступа и своевременное обновление программного обеспечения.

Литература

1. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы. Современные тенденции технических наук: материалы Междунар. науч. конф. — Уфа, 2011. — С. 8-13. — URL: moluch.ru/conf/tech/archive/5/1115/

2. Бабенко Г.В., Белов С.В. Анализ трафика TCP/IP на основе методики допустимого порога и отклонения // Инженерный вестник Дона, 2011, №2 URL: ivdon.ru/ru/magazine/archive/n2y2011/446

3. Factmonster.com. (2019). How Many Online Worldwide? URL: factmonster.com/science/computers-internet/how-many-online-worldwide/

4. Habr.com. (2015). 10 атак на веб-приложения в действии. URL: habr.com/ru/company/ua-hosting/blog/272205/

5. Килюшева, Е. and Гнедин, Е. (2017). Как хакеры атакуют веб-приложения: боты и простые уязвимости. Securitylab.ru. URL: securitylab.ru/analytics/485977.php

6. Черемных, В. (2017). Виды хакерских атак. It-black.ru. URL: it-black.ru/vidy-khakerskikh-atak/

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

7. TAdviser.ru. (2019). Эксперты Лаборатории Касперского назвали общее число хакеров. URL: tadviser.ru/index.php/Статья:Хакеры

8. Semantica.in. (2017). Что такое вредоносный код. URL: semantica.in/blog/chto-takoe-vredonosnyj-kod.html Revisium.com. (2018). Как искать вредоносный код без антивирусов и сканеров. URL: revisium.com/kb/find_malware_without_scanners.html

9. It-click.ru. (2016). Виды хакерских атак на веб-ресурсы. URL: it-click.ru/articles/web-studio/hacking-web-site.aspx

10. Habr.com. (2016). Атака «Man In The Middle» (MITM) в Wi-Fi сети. URL: habr.com/ru/post/249181/

11. Sniffers. (2019). Снифферы. Anti-Malware.ru. URL: anti-malware.ru/threats/sniffers [Accessed 29 May 2019].

12. Infobezlikbez.ru. (2019). Снифферы (сетевые анализаторы) - ИнфоБезЛикбез. URL: infobezlikbez.ru/ataki/setevye-ataki/247-sniffery-setevye-analizatory

13. Хакер (2018). Актуальные методы спуфинга в наши дни. URL: xakep.ru/2013/10/16/relevant-spuffing/

14. Avast.ru. (2018). Что такое спуфинг и как от него защититься. URL: avast.ru/c-spoofing

15. Anti-Malware.ru. (2018). Все об атаке «Человек посередине» (Man in the Middle, MitM). URL: anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack

16. Kaspersky Lab. (2018). Распределенные сетевые атаки / DDoS. URL: kaspersky.ru/resource-center/threats/ddos-attacks

17. ArduinoKit. (2017). Что такое отказ в обслуживании DoS / DDoS? URL: arduinokit.ru/computers/administration-of-computers/chto-takoe-otkaz-v-obsluzhivanii-dos-ddos.html

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

18. Mentsiev A.U., Dzhangarov A.I. VoIP security threats // Инженерный вестник Дона, 2019, №1 URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

19. Positive Technologies. (2016). Атаки на веб-приложения. URL: ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf

References

1. Borshevnikov A.Ye. Sovremennyye tendentsii tekhnicheskikh nauk: materialy Mezhdunar. nauch. konf. Ufa, 2011. pp. 8-13. URL: moluch.ru/conf/tech/archive/5/1115/

2. Babenko G.V., Belov S.V. Inženernyj vestnik Dona (Rus). 2011, №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/446

3. Factmonster.com. (2019). How Many Online Worldwide? URL: factmonster.com/science/computers-internet/how-many-online-worldwide/

4. Habr.com. (2015). 10-atak na veb-prilozheniya v deystvii [10 attacks on web applications in action]. URL: habr.com/ru/company/ua-hosting/blog/272205/

5. Kilyusheva Ye. and Gnedin Ye. (2017). Kak khakery atakuyut veb-prilozheniya: boty i prostyye uyazvimosti [How hackers attack web applications: bots and simple vulnerabilities.]. Securitylab.ru. URL: securitylab.ru/analytics/485977.php

6. Cheremnykh, V. (2017). Vidy khakerskikh atak [Types of hacker attacks]. It-black.ru. URL: it-black.ru/vidy-khakerskikh-atak

7. TAdviser.ru. (2019). Eksperty Laboratorii Kasperskogo nazvali obshcheye chislo khakerov [Kaspersky Lab experts have named the total number of hackers]. URL: tadviser.ru/index.php/

8. Semantica.in. (2017). Chto takoye vredonosnyy kod [What is malicious code]. URL: semantica.in/blog/chto-takoe-vredonosnyj-kod.html

9. Revisium.com. (2018). Kak iskat' vredonosnyy kod bez antivirusov i skanerov [How to search for malicious code without antiviruses and scanners]. URL: revisium.com/kb/find_malware_without_scanners.html

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

10. It-click.ru. (2016). Vidy khakerskikh atak na veb-resursy [Types of hacker attacks on web resources]. URL: it-click.ru/articles/web-studio/hacking-web-site.aspx

11. Anti-Malware.ru (2019). Sniffers. URL: anti-malware.ru/threats/sniffers [Accessed 29 May 2019].

12. Infobezlikbez.ru. (2019). Sniffery (setevyye analizatory) [Sniffer (network analyzers)]. InfoBezLikbez. URL: infobezlikbez.ru/ataki/setevye-ataki/247-sniffery-setevye-analizatory

13. Khaker (2018). Aktual'nyye metody spufinga v nashi dni [Actual methods of spoofing today]. URL: xakep.ru/2013/10/16/relevant-spuffing/

14. Avast.ru. (2018). Chto takoye spufing i kak ot nego zashchitit'sya [What is spoofing and how to protect against it]. URL: avast.ru/c-spoofing

15. Anti-Malware.ru. (2018). Vse ob atake "Chelovek poseredine" (Man in the Middle, MitM) [All about the attack «Man in the middle» (Man in the Middle, MitM)]. URL: anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack

16. Kaspersky Lab. (2018). Raspredelennyye setevyye ataki. DDoS [Distributed network attacks. DDoS]. URL: kaspersky.ru/resource-center/threats/ddos-attacks

17. ArduinoKit. (2017). CHTO takoye otkaz v obsluzhivanii DoS / DDoS? URL: arduinokit.ru/computers/administration-of-computers/chto-takoe-otkaz-v-obsluzhivanii-dos-ddos.html

18. Mentsiev A.U., Dzhangarov A.I. Inženernyj vestnik Dona (Rus). 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

19. Positive Technologies. (2016). Ataki na veb-prilozheniya [Attacks to web applications]. URL: ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019