Защита периметра цифровой безопасности в эпоху массового сканирования Сети

Арсений Великород

Аннотация
В статье систематизированы векторы атак для большинства категорий интернет-хостов, приведены типичные примеры (RDP BlueKeep, уязвимости WinBox, CUPS и др.), обсуждены роль открытого ПО и массовых сканеров, а также практики защиты: грамотная организация удалённого доступа, осторожность с внешними носителями, своевременные обновления и повышение компьютерной и сетевой культуры.

Ключевые слова:
сетевая безопасность, вредоносы, сканирование Интернета, уязвимость.

Сегодня, несмотря на окончание ресурса свободной IPv4-адресации и весьма слабое развитие IPv6, число устройств, имеющих доступ в глобальную Сеть, не перестаёт расти. Кроме того, сама жизнь всё больше интегрируется с сервисами, доступными через Интернет. Вместе с этим, конечно, растёт и поле возможных злонамеренных действий — взломов, несанкционированного доступа к информации и управлению. В отличие от эпохи начала 90-х, когда вирусы были немногочисленны, сегодня в арсенале злоумышленников находится широкая гамма инструментов, которые имеют не только техническую природу, но в том числе и социальную (т.н. человеческий фактор). В этой статье, не претендуя на исчерпание проблематики, автор попытался, как минимум, систематизировать возможные векторы действия «зловредов» в сети Интернет и напомнить ставшие классикой некоторые правила работы в Сети, которые, увы, сегодня не все и не всегда помнят.

Прежде всего приведём основные актуальные на сегодня категории объектов атак в Интернете (т.е. хостов). Это видится необходимым ввиду того, что реализуемость атак подчас зависит именно от программного «форм-фактора» устройства-хоста. Предлагается следующее деление на категории:

- полноценные операционные системы (серверы и рабочие станции);
- сетевое оборудование;
- IoT (в том числе камеры, «умный дом», встроенные системы и т.п.).

В разрезе этих категорий далее и будет выстраиваться анализ. Следует сказать, что для всех трёх категорий существует один общий и во многом решающий фактор, который делает возможными или невозможными атаки и проникновение зловредов в ПО устройств (т.е. превращение устройств в злонамеренных агентов — части возможных «ботнетов»), — это качество кода в смысле следования в нём общим принципам безопасного программирования. И здесь имеются в виду основные правила, которые известны каждому, кто когда-либо занимался созданием софта: контроль длины записи в буфер и вообще контроль входящих от пользователя данных, использование механизмов, которые позволяют предотвратить атаки, основанные на состоянии блокировки в протоколах [1], а также возможность самому пользователю создавать ситуации, способствующие лёгкому несанкционированному доступу к его устройству (слабые или типовые пароли, оставление фабричного пароля и т.п.).

Сделаем короткий обзор основных моментов, которые делают возможными атаки на хосты в каждой из категорий.

Для ОС семейства Windows на сегодня известно множество векторов атак, основанных на уязвимостях внешних протоколов коммуникации как средства проникновения и захвата привилегированного доступа к системе с правами администратора в результате внутренних уязвимостей в реализации системных служб. Чаще всего последние вызваны возможностью записи за пределами буфера, а также относительно лёгким доступом к записи произвольных данных в память процесса.

В этом плане WinAPI делает «подарок» для злоумышленников, вводя с версии Windows XP функцию WriteProcessMemory [2]. При наличии привилегированного доступа к системе она открывает широкие возможности для запуска произвольного кода изнутри легального исполняемого кода. Такой подход можно встретить в нескольких фреймворках spyware, разработанных в АНБ и ЦРУ и обнародованных WikiLeaks.

Стоит отметить, что в последние годы проблемы с безопас-

ностью исполняемого кода от самой Microsoft становились причиной массовых сбоев в работе их ПО по всему миру, нередко связанных с инфицированием вирусами и сетевыми червями, которые используют обнаруженные уязвимости в коде. Здесь стоит вспомнить уязвимость в протоколе RDP BlueKeep [3], обнаруженную в 2019 году, которая сделала возможным инфицирование множеств систем Windows в т.ч. серверных. Последствия этих атак были во многом катастрофическими т.к. в основном заражение производилось вирусами-шифровальщиками, что приводило к потере данных, с которыми работал бизнес.

Переходим к обзору **для ОС Linux**. Здесь основным носителем уязвимостей является стороннее ПО. И если говорить о самом распространённом способе внедрения, то им остаётся небезопасный код веб-фреймворков, таких как Drupal, WordPress и т.п. Через небезопасные места в коде этих фреймворков злоумышленники подчас не только превращают серверы в части своих ботнетов, но и полностью берут доступ к ним под свой контроль. Конечно, после такого вторжения у владельцев серверов остаётся единственный путь — переустановка ОС.

В стороне, но совсем не забытыми остаются и программные продукты-«старожилы» экосистемы Linux. Так, например, в прошлом 2024 году обнаружился ряд критических уязвимостей в ПО сервера печати CUPS [4]. Уже в этом году стало известно об уязвимостях в некоторых дистрибутивах, которые позволяют несанкционированно получить привилегии root [5].

В целом в последнее время в мире Linux сложилась тенденция, характерная для популярного и динамично развивающегося ПО — развивается как сама операционная система, так и продукты под неё, ведётся как разработка новых продуктов, так и исследование кода существующего ПО. Поэтому, в отличие от эпохи начала взлёта Linux, где система и ПО оставались нишевыми, сегодня, с появлением зрелых коммерческих дистрибутивов и программного обеспечения под них, ситуация с безопасностью кода начнет меняться по образу того пути, который прошли компоненты Windows и ПО для неё.

Однако, не только полноценные серверы и рабочие станции сегодня подвержены атакам со стороны зловредов в Сети. Если не на равном, то хотя бы на сопоставимом уровне в зоне риска находится сегодня и **сетевое оборудование**.

Более всего уязвимы домашние роутеры. Довольно часто их пользователи-владельцы непреднамеренно подвергают опасности свои роутеры и устройства домашней сети, открывая бесконтрольный доступ к службам и интерфейсам устройств, которые совершенно для того не предназначены (отсутствие аутентификации, стойкой к взлому, или небрежно написанный код приводят иногда даже к взлому самого роутера). В этом плане особую роль играет человеческий фактор, хотя известны не единичные случаи нахождения уязвимостей в веб-интерфейсах управления роутерами, а также в некоторых других протоколах управления ими.

Особенно показательным случаем является обнаружение в 2018 году уязвимости в проприетарном протоколе коммуникации между утилитой WinBox и роутерами Mikrotik [6], которые всё чаще сегодня используются как домашние. В результате этой уязвимости, при определенных условиях, стало возможно получить доступ целиком к управлению роутера и произвольно менять его настройки. Позже, в 2023 году, была выявлена другая [7] уязвимость.

В целом, даже не стоит уточнять, насколько опасным является факт неограниченного доступа к веб-интерфейсу любого домашнего маршрутизатора. Возможность взлома устройств при этом возрастает в разы, прежде всего, из-за неприспособленности таких интерфейсов к нахождению в открытом неконтролируемом доступе в Интернете.

Надо сказать, что в этом плане оказываются беззащитны и вполне серьёзные продукты, предназначенные для операторов связи. Так, в 2023 году была обнаружена уязвимость [8] маршрутизаторов под управлением IOS XE, которая предоставляла возможность «без прохождения аутентификации получить полный доступ к системе с максимальным уровнем привилегий, при наличии доступа к сетевому порту, через который функционирует веб-интерфейс». Ранее обнаруживались также и уязвимости в реализации протоколов SNMP [9] и CMP [10].

В этом смысле в ещё более сложной ситуации находится вопрос безопасности для **устройств Интернета вещей**. Ведь чаще всего их аппаратная часть обладает ещё более скромными характеристиками по сравнению с оборудованием связи, что, собственно, налагает вполне очевидные ограничения на их программные возможности (любые программные возможности требуют дополнительного исходного кода, а значит, и пространства на ПЗУ для хранения бинарного исполняемого файла). Чаще всего код программного обеспечения «интернет-вещей» заточен под их вычислительные характеристики в ущерб безопасности. Взлом камер, регистраторов, контроллеров умных домов, встроенных систем и даже IPMI серверов — это не редкость.

Всё это показывает, что любое устройство, доступное из Интернета и имеющее хоть какую-то значимую по сложности интеракцию с неограниченным числом пользователей, не может быть гарантированно защищено от несанкционированного доступа и взлома через уязвимости с помощью «простых защит» вроде более сложного пароля. Сегодня, когда сложность как программного обеспечения, так и взаимодействия его компонентов между собой растёт, перед разработчиками и тестировщиками встают задачи по тестированию их продуктов, по сложности эквивалентные сложности самого кода.

В этой ситуации изначальным моментом любой защиты от «зловредов», взлома и несанкционированного доступа должна стать компьютерная и сетевая грамотность — минимальные практические представления о том, как функционирует Интернет и какие угрозы сегодня существуют в нём для любого хоста. Сегодня практически каждый хост-мастер (специалист, который обслуживает и производит настройку веб-серверов) знает, что как только веб-сервер становится доступным в Сети, уже буквально через сутки он обнаруживается множеством сетевых сканеров, которые, как в целях вполне безобидных (PaloAlto, например, регулярно сканиру-

ет Интернет — скорее всего, для обновления каких-то своих баз безопасности), так и вполне злонамеренных — с целью обнаружения старых уязвимых версий веб-фреймворков, небезопасных словарных паролей, неаккуратно оставленных файлов с дефолтными настройками — сканируют круглосуточно всё адресное пространство Интернета.

Поэтому нужно осознавать, что сама по себе информация о новых версиях и поправленных в них «багах» и уязвимостях прошлых версий (файлы RELEASE и BUGS, поставляемые в комплекте с установочными файлами) — это информация сразу для двух сторон: для тех, кто пользуется программным обеспечением, и для тех, кто ищет уязвимости в нём для злонамеренных действий на чужой инфраструктуре. В эпоху ПО с открытым исходным кодом (если взять несколько шире — в эпоху легкодоступных открытых данных) все эти данные более не являются тайной. Следует вполне серьёзно брать в расчёт возможность того, что эти данные могут быть и будут использованы в целях не вполне благонамеренных — для поиска тех, кто ещё использует WordPress старой версии с уязвимостью, или тех, кто оставил файл с паролем пользователя admin в веб-директории с возможностью его чтения всеми пользователями.

Какие основные моменты обеспечения безопасности можно упомянуть в рамках статьи? В отношении организации удалённого доступа к ресурсам домашней или корпоративной сети следует сказать, что вопрос всегда состоит в разумном компромиссе между техническими возможностями сетевой инфраструктуры, удобством доступа и управления им. Причём этот выбор всегда зависит в равной степени как от возможностей сетевого оборудования (маршрутизатора или файервола), так и от характеристик ресурса внутренней сети и протоколов доступа к нему.

И выбор здесь действительно широк. В плане технологии доступа обычно возможны: прямой доступ через веб, ограничение списками доступа (ACL), проброс портов, ssh-тунель, разнообразные типы VPN и т.п. С точки зрения самого ресурса, также возможны разные варианты доступа, причём порой одновременно несколько. И, в конечном итоге, разумное решение этого действительно комплексного вопроса во многом зависит от осведомлённости хозяев инфраструктуры о том, какие сетевые ресурсы возможно выставлять «голым» интерфейсом в Интернет, а какие нет; какие риски, неудобства и преимущества несёт то или иное решение по доступу к ним.

Надо сказать, что оценка пригодности интерфейсов для нахождения в среде открытого публичного доступа в Интернете является самостоятельной задачей. Как понять, что можно оставлять без условного ACL, а к чему возможен доступ только через VPN с IPSEC? Конечно, в первую очередь, примитивные соображения об уровне доступа, который может получить потенциальный взломщик в случае взлома. Но, как было сказано ранее, есть и менее очевидные моменты. В какой степени реализация того же веб-интерфейса является безопасной? Ответ на этот вопрос далеко не тривиален. Ведь есть ситуации, когда возможность SQL-инъекций или внедрения шелл-кодов совершенно не очевидна обычному пользователю. Чтобы узнать это, часто необходим анализ кода приложения на уровне опытного программиста. И эта задача становится действительно ещё сложнее, если приложение запускается в embedded-окружении. В рамках этой статьи совершенно не представляется возможным подробно рассмотреть этот вопрос. Однако следует подчеркнуть его значимость для обеспечения устойчивого периметра безопасности.

Переходя к более простым вещам, не обойдём вниманием и безопасность паролей. К сожалению, этот вопрос и в наши дни далёк от решения. Автору статьи не раз приходилось видеть несерьёзное отношение к сложности пароля или к вопросу его сохранения в тайне. А ведь пароль тем и ценен, что в идеале он известен только одному человеку. Ещё хуже сегодня ситуация с применением тактики периодической смены паролей. Сегодня уже понятно, что эта тактика требует определённой переоценки, т.к. иногда или нереализуема вообще, или вырождается в побочные проблемы безопасности. Современные возможности перебора паролей дают широкие возможности для того, чтобы совершить подбор в умеренные сроки, особенно если мы говорим о персистирующих сетевых червях и ботнетах. Поэтому, чем дальше используемый пароль от «словарных наборов», тем сложнее произвести его подбор. Увы, возможности злоумышленников в современных реалиях осознаются далеко не всеми. И несмотря на масштабное развитие методов «социальной инженерии» (фишинг и ему подобное), словарный подбор продолжает занимать совсем не последнее место в обойме доступных методов несанкционированного доступа к системам и данным.

Последними в очереди, но первыми по значимости идут старые как мир предостережения об осторожности при использовании чужих флешек. Ведь именно они довольно часто являются носителями вредоносных программ. Также стоит избегать неконтролируемого доступа третьих лиц к персональным компьютерам и информации, хранящейся на них. Желательно, чтобы чувствительная информация не хранилась в незашифрованном виде. Это позволяет, при определённых условиях, сделать её резервные копии и держать на внешнем хранилище (иногда даже облачном).

Завершая статью, следует сказать, что своевременное обновление программного обеспечения и компонентов операционных систем является также одним из моментов безопасности. Конечно, и здесь не стоит проявлять маниакального рвения накатить каждое обновление. Всё же, чаще всего сегодня возможно чётко определить критичность обновления, и ограничиться только самыми необходимыми.

Несомненно, столь обширный вопрос, как сетевая безопасность в эпоху всеобщей интернетизации и открытого доступа, невозможно охватить одной или даже несколькими статьями. А если учитывать всё многообразие ситуаций, то, наверное, можно написать целый учебник на эту тему. Однако взломы, заражения сетевыми червями, шпионскими вредоносами, а также утечки информации происходят в последнее время всё чаще. Поэтому необходимо подчеркнуть, что эпоха относительной безопасности Интернета в смысле пассивности угроз в нём закончилась. Сегодня как от профессионалов, так и от обычных пользователей требуется всё больше и больше знаний, чтобы сохранять свои данные в безопасности, а частную жизнь и корпоративные данные

неприкосновенными. И в этом обзоре автор постарался подсветить технологический охват и сложность проблемы сетевой безопасности в современных реалиях.

Список литературы:

[1] Пример пентеста, основанного на проверке возможности такой атаки: https://github.com/pentestfunctions/CVE-2024-6387/blob/production/7etsuo-regreSSHion.c

[2] https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-writeprocessmemory

[3] https://www.securitylab.ru/blog/company/PandaSecurityRus/346879.php

[4] https://habr.com/ru/companies/spring_aio/articles/846498/

[5] https://www.securitylab.ru/news/563447.php https://cloudsecurityalliance.org/blog/2023/10/17/new-container-exploit-rooting-non-root-containers-with-cve-2023-2640-and-cve-2023-32629-aka-gameover-lay#

[6] https://habr.com/ru/articles/416067/ , https://habr.com/ru/articles/359038/

[7] https://habr.com/ru/news/750608/

[8] https://www.opennet.ru/opennews/art.shtml?num=59948

[9] https://www.opennet.ru/opennews/art.shtml?num=46868

[10] https://www.opennet.ru/opennews/art.shtml?num=46522

Об авторе

Великород Арсений Валентинович,
старший сетевой инженер CDN-Video,
ORCID: https://orcid.org/0009-0003-6549-8292