УДК 004.738.5
ББК 32.973.202
Г85

The Great Firewall of China:
How to Build and Control an Alternative Version of the Internet
by JAMES GRIFFITHS

Художественное оформление *Алексея Шуклина*

Гриффитс, Джеймс.

Г85 Великий Китайский Файрвол / Джеймс Гриффитс ; [перевод с английского Н. А. Комар, А. В. Ефимовой]. — Москва : Эксмо, 2022. — 464 с. — (Кругозор Дениса Пескова).

ISBN 978-5-04-108636-7

Представьте, что вы оказались в мире без интернета. Некуда загрузить фотографию, не с кем поделиться смешной картинкой, негде быстро получить нужную информацию. Кажется, что сегодня такое практически невозможно, но иногда это результат единственного решения и нескольких нажатий на кнопку.

Интернет начинался как развиваемый энтузиастами островок свободы, но с тех пор им научились управлять — как государства, так и крупные корпорации. Фраза «интернет помнит все» обрела второй смысл — контент стал подконтролен, иллюзия анонимности исчезла, а любое неосторожное сообщение может создать массу трудностей автору. Книга рассказывает о том, как Китай первым в мире научился управлять интернетом и как другие страны перенимали его опыт.

УДК 004.738.5
ББК 32.973.202

ISBN 978-5-04-108636-7

СОДЕРЖАНИЕ

«Западные силы, настроенные против Китая, постоянно используют интернет, чтобы, как они говорят, свалить нас, и постоянно терпят поражение... То, насколько мы сможем отстоять свои интересы и победить в этой битве за интернет, напрямую скажется на идеологической и политической безопасности нашей страны».

Си Цзиньпин, из выступления
на Рабочей конференции по национальной
идеологии и пропагандистской работе,
август 2013 г.

СПИСОК СОКРАЩЕНИЙ

BBG	Broadcasting Board of Governors (Наблюдательный совет по международному вещанию)
CDA	Communications Decency Act (Закон о соблюдении пристойности в телекоммуникациях)
CNC	компания China Netcom Communications
DARPA	Defence Advanced Research Projects Agency (Управление перспективных исследовательских проектов Министерства обороны США)
DDoS	распределенная атака типа «отказ в обслуживании», распределенная DoS-атака
DIT	компания Dynamic Internet Technology Inc.
DNS	сервер(ы) доменных имен
DPI	глубокий анализ пакетов
EFF	Electronic Frontier Foundation (Фонд электронных рубежей)
GIFC	Консорциум глобальной интернет-свободы
IANA	Internet Assigned Numbers Authority (Администрация адресного пространства интернета)

ICANN	Корпорация по управлению доменными именами и IP-адресами
IETF	Internet Engineering Task Force (Инженерный совет интернета)
IP	интернет-протокол
LAN	локальная вычислительная сеть
NED	National Endowment for Democracy (Национальный фонд демократии)
URL	единый указатель ресурса
VPN	виртуальная частная сеть
W3C	Консорциум Всемирной паутины
WELL	Whole Earth 'Lectronic Link (Всепланетная электронная связь)
WSIS	Всемирный саммит по вопросам информационного общества
АНБ	Агентство национальной безопасности
ВТО	Всемирная торговая организация
ВУК	Всемирный уйгурский конгресс
КГБ	Комитет государственной безопасности
КДП	Китайская демократическая партия
КНИИЦ	Китайский научно-исследовательский институт цигун

Список сокращений

КНР	Китайская Народная Республика
МПИ	Министерство промышленности и информатизации КНР
МСЭ	Международный союз электросвязи
НОАК	Народно-освободительная армия, вооруженные силы Коммунистической партии Китая и Китайской Народной Республики
СОРМ	система оперативно-розыскных мероприятий
ФАПСИ	Федеральное агентство правительственной связи и информации
ФСБ	Федеральная служба безопасности
ШОС	Шанхайская организация сотрудничества

Карта Китая, спорных территорий и специальных административных округов (Китайская Народная Республика, Гонконг, Тайвань, Макао)

Введение
ПЕРВЫЕ СИМПТОМЫ

Однажды в среду, в марте 2015 года в офисе IT-компании GitHub в Сан-Франциско прозвучала тревога. Древесный массив, много свободного места и естественного света — в общем, в помещениях компании господствовал тот самый бездушный скандинавский стиль, моду на который ввели в Кремниевой долине. Под сводом из мощных деревянных балок и алюминиевых воздуховодов барабанили по клавишам инженеры. Кто-то уже вышел из здания, но большинство еще собирались по домам. На улице стояла теплая ясная погода. Солнце только начинало садиться.

Сигнал тревоги не был для сотрудников GitHub чем-то из ряда вон выходящим. Для компании с 14 миллионами пользователей, на серверах которой хранился крупнейший в мире репозиторий компьютерного кода, жизненно важно, чтобы сервис был доступен круглосуточно и ни на секунду не выходил из строя. Разработчики в крупных и мелких компаниях по всему миру пользуются кодом на GitHub, каждую минуту тысячи пользователей загружают проекты, отмечают уязвимости и баги, выпускают новые версии программ и приложений. Короче говоря, если GitHub упадет, об этом будут знать все.

Первое тревожное сообщение было о том, что по нескольким проектам на GitHub зафиксированы большие объемы входящего трафика. Причина могла быть в чем угодно: от выпуска крупного обновления до

чего-то гораздо более серьезного. При увеличении объемов трафика, угрожающего функционированию сервиса, выдавались бы новые тревожные сообщения.

В тот день так и случилось. Серверы GitHub обрушились из-за DDoS-атаки[1].

Чаще всего сайты «ложатся» из-за внезапного притока трафика. Не в силах обработать множество одновременно входящих запросов, серверы выходят из строя или переключаются на черепашью скорость. Например, в 2015 году сайт Эйфелевой башни упал из-за того, что в дудл Google в честь 126-й годовщины постройки башни была вставлена соответствующая ссылка, по которой одновременно перешли миллионы посетителей[2]. По такому же принципу устроена DDoS-атака, но при этом она всегда кем-то инициирована. В последнее время количество таких атак увеличивается по экспоненте с ростом числа ботнетов, или армии компьютеров-зомби, инфицированных вирусным кодом, с помощью которого хакеры осуществляют над ними удаленный контроль.

«GitHub стал жертвой крупнейшей DDoS-атаки в своей истории», — так почти через сутки после начала атаки написал в своем блоге главный разработчик компании Джесси Ньюленд[3]. Если судить по имеющимся в открытом доступе сообщениям о статусе серверов, в течение следующих пяти дней сервер GitHub падал девять раз[4]. Инженеры сервиса 120 часов пытались отразить атаку, а она, как гидра, приспосабливалась и становилась вдвое сильнее, как только казалось, что с ней удалось справиться. В компании GitHub отказались от официальных комментариев, но один сотрудник на условиях анонимности сказал мне: «с таким мы еще никогда не сталкивались».

Во внутреннем чате GitHub сотрудники делились опасениями, что с атакой придется разбираться еще

какое-то время. Была одна проблема: все использованные ими ранее методы подбирались под атаки, с которыми GitHub и другие компании уже имели дело. А эта атака была другой. Счет шел уже не на часы, а на сутки. Между инженерами GitHub и неизвестными организаторами атаки развернулось что-то вроде соревнования. Напряженная сверхурочная работа не оставляла команде GitHub времени подумать, кто скрывается за маской хакеров. Комментируя слухи, плодившиеся в интернете, представители GitHub повторяли: «Мы считаем, что цель атаки — заставить нас убрать с сайта определенный контент».

Николас Уивер, житель Беркли, университетского городка в двадцати минутах езды от Сан-Франциско, был уверен, что знает, кто стоит за атакой, — Китай. Уивер, лысеющий мужчина в очках, всегда ходит в рубашке поло, говорит четко и по делу. Когда-то он был астрофизиком, но потом заинтересовался компьютерной безопасностью. Сперва атака на GitHub не привлекла его внимания. Сайты компаний подвергаются DDoS-атакам чуть ли не каждый день, да и GitHub уже сталкивалась с ними не раз. Но в интернете начали обсуждать, кто может быть неизвестным злоумышленником, и Уивер заинтересовался. Общаясь с другими экспертами по кибербезопасности в Twittere и блогах[5], он сузил радиус атаки до двух конкретных проектов на GitHub. Оба были связаны с GreatFire.org. Это китайская организация по противостоянию национальной интернет-цензуре. Выложенные на GitHub разработки предоставляли пользователям на территории Китая доступ к двум сайтам из черного списка — собственно сайту GreatFire и китайской версии сайта New York Times. GreatFire также входит в список иностранных антикитайских организаций по версии Управления по вопросам киберпространства КНР[6]. Сайт организации

уже давно подвергалась массированным DDoS-атакам и взломам. Поэтому ей пришлось перенести часть сервисов на GitHub, где они, по идее, должны были оказаться вне досягаемости.

Анализируя атаку, Уивер обнаружил доселе неизвестные элементы, которые могли иметь масштабные последствия для кибербезопасности. Совместно с Биллом Марчаком и еще семью исследователями в издательстве лаборатории Citizen Lab при Университете Торонто Уивер опубликовал работу, в которой утверждалось, что Китай разработал беспрецедентное кибероружие под названием «Большая пушка» (Great Cannon). Исследователи Citizen Lab проследили «Большую пушку» до инфраструктуры, которую использует Великий файрвол. Это гигантский аппарат интернет-цензуры, который отделяет интернет Китая от остального мира и контролирует, какие данные могут получать и передавать пользователи внутри страны.

«Факт успешного применения „Большой пушки“ представляет собой значительное достижение в области управления информацией на государственном уровне, — говорится в работе. — Цензура осуществляется путем передачи инструмента атаки в руки пользователей и нормализации широкомасштабных атак». Для атаки на GitHub «Пушка» использовала сервисы Baidu, одного из китайских интернет-гигантов. «Пушка» нашла уязвимость в системе онлайн-рекламы Baidu с миллионами показов по всему миру, перехватила трафик и перенаправила его на серверы GitHub. На тот момент сайт Baidu, которая, кстати, всячески отрицала свое участие в атаке, занимал четвертое место в мире по посещаемости. При каждом переходе на сайт с баннерами из системы Baidu код запрашивал данные с китайских серверов компании. Пока запрос обрабатывался, «Пушка» перехватывала фрагменты данных и заменяла