Международный союз электросвязи

МСЭ-Т X.1213

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2017)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи

Рекомендация МСЭ-Т X.1213

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальный трансапортных системы (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Протоколы обеспечения безопасности	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1213

Требования к возможностям обеспечения безопасности для противодействия бот-сетям, использующим смартфоны

Резюме

В Рекомендации МСЭ-Т X.1213 приведен анализ текущей ситуации и потенциальных угроз безопасности со стороны бот-сетей, использующих смартфоны, а также требования к возможностям обеспечения безопасности.

Как показывают результаты обследований, проводимых всемирными организациями, наряду с высокими темпами развития устройств мобильного доступа в интернет и широким использованием смартфонов, бот-сети, целью которых ранее были сети на базе персональных компьютеров, теперь довольно быстро тиражируются на смартфонах. В настоящее время в странах и регионах, характеризующихся различными условиями и экосистемами, действуют ограничения разных уровней на распространение бот-сетей, использующих смартфоны. Аналитические отчеты различных компаний, занимающихся вопросами безопасности, и организаций, ведущих расследования, свидетельствуют о заметной разнице в статистических данных, отражающих уровень распространения бот-сетей, использующих смартфоны. В некоторых регионах потенциальная угроза бот-сетей, использующих смартфоны, возрастает весьма высокими темпами и, вероятно, может охватить весь мир, превратившись из регионального вопроса в серьезную глобальную проблему.

По сравнению с персональными компьютерами и серверами, смартфоны обладают меньшей вычислительной мощностью, меньшим объемом памяти и меньшим ресурсом батареи. Однако неблагоприятное воздействие бот-сетей, использующих смартфоны, может иметь более серьезные последствия для пользователей по следующим причинам: 1) в смартфонах часто хранится очень важная информация, позволяющая установить личность (PII); и 2) в случае атаки на смартфоны или на инфраструктуру оператора, пользователь может пострадать существенным образом из-за широкого распространения смартфонов и зависимости пользователей от них.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1213	06.09.2017 г.	17-я	11.1002/1000/13261

Ключевые слова

Бот-сеть, контроль и управление (C&C), вредоносное ПО, информация, позволяющая установить личность (PII), смартфон.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1213

Требования к возможностям обеспечения безопасности для противодействия бот-сетям, использующим смартфоны

1 Сфера применения

Настоящая Рекомендация содержит требования возможности обеспечения безопасности для противодействия бот-сетям, использующим смартфоны. Целью данной Рекомендации является изучение проблем, связанных с бот-сетями, использующими смартфоны, конкретных угроз, которые они представляют для сетей операторов и самих смартфонов, а также требований к их безопасности. Основное внимание уделяется анализу угроз и перечислению требований. Цель – защита инфраструктуры операторов и смартфонов, обеспечение гарантированного и качественного обслуживания, а также повышение уровня удобства работы пользователей. Рассмотрение конкретных технических решений и других интеллектуальных терминалов, таких как планшетные устройства, выходит за рамки настоящей Рекомендации.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 бот (bot) [b-ITU-T X-Sup.8]: Автоматизированное программное обеспечение, которое используется для выполнения конкретных задач, предназначенных для достижения злонамеренных целей. Этот термин является синонимом термина "робот".

3.1.2 владелец ботов (botmaster) [b-ITU-T X-Sup.8]: Лицо, ответственное за управление и обслуживание бот-сети.

3.1.3 бот-сеть (botnet) [b-ITU-T X-Sup.8]: Дистанционно управляемые вредоносные программные роботы (боты), которые автономно или автоматически запускаются на зараженных компьютерах вместе с командно-управляющим сервером, принадлежащим владельцам бот-сетей.

3.1.4 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ITU-T X.1252]: Любая информация, a) которая идентифицирует или может использоваться для идентификации, установления контакта или определения местонахождения лица, к которому относится такая информация; b) из которой может быть получена идентификационная или контактная информация физического лица, или c) которая прямо или косвенно связана или может быть связана с физическим лицом.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Принятые сокращения

В настоящей Рекомендации используются следующие сокращения и акронимы:

2G	Second Generation of mobile telecommunication	Технология подвижной электросвязи второго поколения
2FA	Two Factor Authentication	Двухфакторная аутентификация
3G	Third Generation of mobile telecommunication	Технология подвижной электросвязи третьего поколения

4G	Fourth Generation of mobile telecommunication		Технология подвижной электросвязи четвертого поколения
API	Application Programming Interface		Интерфейс прикладного программирования
C&C	Command and Control		Контроль и управление
CPU	Central Processing Unit	ЦП	Центральный процессор
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
DNS	Domain Name System		Система наименований доменов
GPS	Global Positioning System		Глобальная система определения местоположения
HTTP	Hyper Text Transfer Protocol		Протокол передачи гипертекста
IDS	Intrusion Detection System		Система обнаружения вторжений
IoT	Internet of Things		Интернет вещей
IP	Internet Protocol		Протокол Интернет
IPS	Intrusion Prevention System		Система предотвращения вторжений
MITM	Man-in-the-Middle		Посредник
MMS	Multimedia Messaging Service		Услуга передачи мультимедийных сообщений
NFC	Near Field Communication		Связь ближнего действия
OTP	One-Time Passcode		Одноразовый пароль
P2P	Peer-to-Peer		Одноранговый протокол
PC	Personal Computer	ПК	Персональный компьютер
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PNG	Portable Network Graphic		Переносная сетевая графика
QoS	Quality of Service		Качество обслуживания
QRcode	Quick Response code		Код быстрого ответа
SIM	Subscriber Identity Module		Модуль идентификации абонента
SMS	Short Message Service		Услуга передачи коротких сообщений
USB	Universal Serial Bus		Универсальная последовательная шина
Wi-Fi	Wireless Fidelity		Беспроводной интернет

5 Условные обозначения и соглашения по терминологии

Отсутствуют.

6 Введение

Наряду с быстрым развитием мобильных интернет-устройств мобильные терминалы становятся все более интеллектуальными, обладающими более высоким уровнем возможностей. В настоящей Рекомендации термин "смартфон" относится к мобильным телефонам со следующими характеристиками:

- независимая операционная система;
- способность к постоянному расширению функций и возможностей телефона посредством установки сторонних приложений;
- возможность доступа к беспроводной сети, в том числе к мобильному интернету через сеть оператора подвижной электросвязи.

В последние годы число пользователей смартфонов стремительно растет. Смартфоны обеспечивают людям удобство, но в то же время для них возрастает угроза безопасности.

6.1 Обзор вопросов безопасности

Учитывая стремительно растущее число пользователей смартфонов, необходимо эффективно подавлять и контролировать бот-сети, использующие смартфоны, с тем чтобы они не стали фактором, влияющим на общественное спокойствие и угрожающим общественной безопасности.

Крупномасштабные бот-сети могут серьезно навредить эффективной эксплуатации сетей операторов подвижной связи и ухудшить качество обслуживания пользователей (QoS), что приведет к неудовлетворенности пользователей и потере абонентов. Ущерб для пользователей, чьи смартфоны были взломаны и контролируются через бот-сети, может быть весьма ощутимым, так на смартфонах часто хранят большой объем важной информации, позволяющей установить личность (PII), такую как списки контактов и информация об онлайн-платежах.

Поэтому работа по противодействию бот-сетям, использующим смартфоны, перспективна и полезна. Для того чтобы подавить быстрый рост числа бот-сетей, уменьшить потери абонентов, сократить количество жалоб и т. д., операторам следует повышать степень своей осведомленности в вопросах безопасности в этой сфере.

6.2 Эволюция угроз бот-сетей для смартфонов

Появление вирусов для смартфонов можно проследить начиная с 2004 года, когда был обнаружен первый червь на базе смартфона – *Cabir*. В 2009 году вредоносное ПО *iKee.B* приобрело характеристики бот-сети и могло брать под контроль инфицированные смартфоны iPhone, передавая владельцу бот-сети PII пользователей. В 2011 году был обнаружен образчик мобильной бот-сети *Android.Geinimi*. Он мог скрывать методы связи, имел большое количество атакующих модулей и был признан чрезвычайно опасным.

Широкое распространение смартфонов сопровождалось необычайным ростом числа вредоносных программ на их базе, которые, как правило, используют в качестве среды распространения те или иные функции смартфона. После загрузки и установки на смартфон такая вредоносная программа часто и тайно отображает рекламные объявления, создает дополнительный трафик смартфона, удерживает плату и т. д., причиняя ущерб пользователю смартфона. Более того, пользователи смартфонов также могут столкнуться с такими проблемами, как направление на фишинговые веб-сайты, заражение смартфона вирусами или троянскими программами, раскрытие или кража списков контактов и/или адресных книг и кража учетных записей и паролей. Чаще всего происходит раскрытие PII, личных счетов и паролей.

В последние годы количество вредоносных программ для смартфонов демонстрирует экспоненциальный рост. Вредоносное ПО является основной причиной распространения вирусов бот-сетей, так как все большая часть вредоносного ПО использует методы или функции дистанционно управляемой лазейки, которые являются отличительной чертой ботов на базе смартфонов. Основная цель владельцев бот-сетей – получение прибыли от кражи PII и незаконных сборов. В настоящее время к наиболее распространенным функциям вредоносных программ относятся: хищение PII, незаконное удержание платы, мошенничество, ухудшение рабочих характеристик и распространение вредоносного ПО.

6.3 Защита смартфонов

Основные проблемы безопасности, с которыми сталкиваются пользователи смартфонов, это навязчивые звонки, спам в виде коротких сообщений (SMS) и другие нарушения безопасности, возникающие в процессе просмотра веб-страниц, загрузки файлов, выполнения мобильных платежей и т. д. Эти угрозы обычно ослабляются программным обеспечением безопасности, установленным на смартфонах.

Две основные функции программного обеспечения безопасности для смартфонов – это управление телефоном и защита. Функция управления телефоном включает в себя очистку памяти, продление времени работы в режиме ожидания, управление программой автоматической загрузки, управление SMS-сообщениями, управление телефонными номерами и т. д. Цель функции управления телефоном – сделать работу смартфона бесперебойной и повысить эффективность использования устройства. Обеспечение защиты, как правило, включает в себя мониторинг трафика данных, блокирование навязчивых звонков, регулярное сканирование, регулярное удаление вирусов и т. д. Цель этой функции – защитить смартфон от угроз для безопасности.

Установка программного обеспечения безопасности помогает защитить смартфон от определенных бот-сетей и вредоносного ПО на стороне пользовательского терминала, но по мере того как злоумышленники совершенствуются, а способы их атак становятся все разнообразнее, смартфоны будут подвергаться усиливающимся угрозам безопасности. Наряду с повышением уровня безопасности на стороне терминала необходимо также, чтобы операторы обеспечили дополнительную защиту на стороне сети. Координация и сотрудничество обеих сторон значительно усилят способность смартфонов противостоять атакам бот-сетей.

7 Характеристики бот-сетей, использующих смартфоны

Бот-сети, использующие смартфоны и интернет для широкого распространения вредоносного ПО, эксплуатируют возможности смартфонов и мобильных сетей. Анализируя эти возможности, а также цели атак владельцев бот-сетей, можно судить о характеристиках бот-сетей, использующих смартфоны, и выявить потенциальные угрозы для безопасности.

7.1 Боты, охотящиеся за информацией, позволяющей установить личность

Бот-сети, использующие смартфоны, состоят из большого числа ботов на основе смартфонов. В отличие от традиционных персональных компьютеров (ПК) в смартфонах хранится большое количество сведений PII и конфиденциальной информации, что делает бот-сети, использующие смартфоны, особенно опасными для пользователей, которые могут ощутимо пострадать из-за потери данных.

В число функций, встроенных в смартфоны, входят: управление персональной информацией, расписание и повестка дня, ежедневник, планирование задач, мультимедийные приложения, просмотр веб-страниц и т. д. Обилие персональной информации, хранящейся в приложениях, делает смартфоны основной целью злоумышленников. Более того, система глобального определения местоположения смартфона (GPS) позволяет получать информацию о местоположении пользователя, которая составляет еще один тип PII. Получив эту информацию, злоумышленники могут раскрыть PII пользователя.

7.2 Различные средства распространения

Во-первых, бот-сети, использующие смартфоны, могут распространяться через зараженные приложения, которые пользователи обычно находят и загружают из магазинов приложений или с пользовательских форумов, где не требуется никакой проверки подлинности.

Во-вторых, бот-сети, использующие смартфоны, могут распространяться через Bluetooth, беспроводной интернет (Wi-Fi), универсальную последовательную шину (USB) и другие периферийные интерфейсы смартфонов.

В-третьих, бот-сети, использующие смартфоны, могут распространяться через протокол передачи гипертекста (HTTP), SMS, услугу передачи мультимедийных сообщений (MMS), код быстрого ответа (QR-код) и т. д.

Разнообразные носители делают распространение бот-сетей, использующих смартфоны, относительно простым делом, что вынуждает предъявлять повышенные требования к защитным средствам обеспечения безопасности.

7.3 Открытость

Открытые мобильные операционные системы гарантируют пользователям смартфонов широкий выбор прикладных программ, но в то же время эти программы увеличивают число потенциальных угроз для смартфонов и уровень опасности атак хакеров. Открытость позволяет хакерам внедрять в расширенные приложения вирусы или трояны, облегчая распространение бот-сетей, использующих смартфоны.

Смартфоны обладают различными типами периферийных интерфейсов: Bluetooth, связь ближнего действия (NFC) и USB. Злоумышленники могут использовать любые соединения на основе этих периферийных интерфейсов. Более того, смартфоны обычно поддерживают доступ к мобильным сетям второго, третьего или четвертого поколения (2G, 3G или 4G), а также сети Wi-Fi, с помощью которых пользователи могут получить доступ к интернету. Эти функции имеют уникальное прикладное и коммерческое значение, но также предоставляют злоумышленникам множество лазеек для атак.

7.4 Целенаправленное заражение

Бот-сети, использующие смартфоны, обычно нацелены на устройства определенного типа и заражают их путем прямого копирования или склонения пользователей к загрузке вредоносного ПО или троянов. Злоумышленники также могут нацеливаться на смартфоны, работающие с одной и той же операционной системой. Этот метод значительно повышает эффективность атак и снижает их стоимость.

7.5 Маскировка

Бот-сети, использующие смартфоны, становятся все более сложными. Некоторые из них способны скрывать свои атаки, удаляя все следы установки после успешного заражения смартфона. Другие, отправив PII пользователя через интернет, могут стереть данные о сетевых соединениях и следы исходящих соединений. Они могут даже заказать специальные услуги конкретных поставщиков и автоматически заблокировать подтверждающие сообщения операторов сетей подвижной электросвязи.

Некоторые троянские и вредоносные программы для смартфонов, которые воруют PII или производят незаконные сборы, начинают свои атаки не сразу после успешной установки. Они выжидают в течение заданного периода времени или используют период бездействия зараженного смартфона.

Сегодня все большая и большая доля вредоносных программ используют в качестве базовой функции дистанционно управляемые лазейки, что служит одной из отличительных особенностей бот-сетей, использующих смартфоны.

Многие бот-сети распространяются через вредоносные программы, встроенные в популярные мобильные приложения. Когда пользователь загружает и устанавливает такие приложения из магазина приложений или с пользовательских форумов, не имеющих защищенных механизмов проверки подлинности, запускаются вредоносные программы, скрытые в таких приложениях.

7.6 Коммерческие интересы

В отличие от большинства традиционных вредоносных программ, целью которых является саботаж, цель бот-сетей, использующих смартфоны, часто состоит в получении прибыли. Например, владельцы бот-сетей, использующих смартфоны, получают прибыль от кражи PII пользователей или от незаконных сборов, таким образом образуя теневую индустрию интернет-мошенничества. Коммерческая прибыль побуждает злоумышленников вкладывать больше ресурсов в разработку бот-сетей на основе смартфонов и способствует развитию этой индустрии интернет-мошенничества. Это означает, что бот-сети, использующие смартфоны, создают все больше угроз для безопасности пользователей, и бороться с такими угрозами будет все труднее.

7.7 Постоянно меняющиеся сетевые соединения

Высокая мобильность смартфонов ведет к постоянному изменению сетевых соединений, что приводит к повышению степени изменчивости бот-сетей, использующих смартфоны. Смартфоны могут перемещаться между сетями, использующими как одни и те же, так и разные сетевые технологии, например из сети 3G в пункт доступа Wi-Fi. Следовательно, боты зараженных смартфонов должны чаще изменять каналы связи с сервером контроля и управления (C&C), чем боты, использующие ПК. Это дополнительно усложняет обнаружение бот-сетей, использующих смартфоны, путем выявления их каналов связи.

8 Угрозы для безопасности

8.1 Раскрытие информации, позволяющей установить личность

– Информация, хранящаяся в модуле идентификации абонента (SIM)

  Когда смартфон заражается ботом, владельцы бот-сети получают возможность красть информацию из модуля идентификации абонента, включая регистрационные данные телефона, параметры конфигурации оборудования и т. д. Они получают ощутимую финансовую выгоду от продажи или раскрытия этой PII. Еще большее беспокойство вызывает возможность владельцев бот-сетей запускать более опасные атаки на смартфоны с одинаковой конфигурацией, анализируя уязвимости этих устройств.

– Память телефона

Владельцы бот-сетей, использующих смартфоны, могут осуществлять дистанционное управление всеми своими ботами из облака. Таким способом владельцы бот-сети получают от бота PII пользователя, включая номер телефона, список контактов, журналы звонков, электронные письма, информацию о местоположении, фотографии и видеозаписи и т. д. Они могут поручить своим ботам загружать всю эту информацию на удаленные серверы.

– Банковские счета и пароли

Когда пользователь совершает платеж посредством смартфона, злоумышленники могут получить полный контроль над смартфоном пользователя, эксплуатируя его уязвимости, а затем украсть номера банковских счетов и пароли. Более того, злоумышленники могут перехватывать SMS с кодом подтверждения и инициировать незаконные денежные переводы, стерев все следы атаки. Этот способ позволяет злоумышленникам легко красть деньги без ведома пользователя смартфона.

– Учетные записи и пароли приложений

Точно так же злоумышленники могут красть учетные записи и пароли пользователей приложений. Эту информацию можно применять для совершения дальнейшего мошенничества и получения соответствующей прибыли.

8.2 Незаконное снятие средств расходования

– Автоматическая загрузка или удаление программного обеспечения

Когда смартфон контролируется ботом, он получает инструкции от C&C-сервера, и владелец бот-сети может дать телефону команду на выполнение почти любой операции. По указанию владельца бот-сети смартфон может автоматически загружать или удалять приложения. Это чревато повышенными расходами на потребление трафика и финансовыми потерями для пользователя.

– SMS-спам

Некоторые вредоносные программы могут заставить смартфон рассылать SMS-спам по номерам из списка контактов. Сначала злоумышленник, обманув пользователя, загружает и устанавливает на смартфон вредоносное ПО, после чего тот автоматически связывается с C&C-серверами для получения инструкций. Получив инструкции по рассылке SMS-спама, смартфон рассылает SMS-сообщения по номерам из своего списка контактов, что приводит к снижению производительности и удержанию платы за доступ в интернет и отправку SMS-сообщений. Интенсивный SMS-спам забивает каналы подвижной связи, что ведет к снижению производительности и к недоступности смартфона. Более того, если взломанный смартфон принадлежит компании или государственному учреждению, то их репутация может быть подорвана, поскольку список контактов, хранящийся в смартфоне, может содержать телефоны важных деловых партнеров или должностных лиц. Если от зараженного смартфона часто приходит SMS-спам, получатель может занести его номер в черный список, что приведет к непредсказуемым финансовым потерям и ущербу для делового сотрудничества.

8.3 Неправомерное поведение

– Распределенные атаки типа "отказ в обслуживании" (DDoS)

Благодаря широкому использованию смартфонов и быстрому росту числа мобильных интернет-приложений, когда число контролируемых ботов очень велико, владельцы бот-сетей могут организовывать DDoS-атаки. Они могут контролировать большое количество зараженных смартфонов и запускать со специального веб-сайта одновременные атаки, приводящие к отказам веб-серверов. В частности, если взломанные смартфоны принадлежат определенным компаниям или государственным учреждениям, их репутация может быть в значительной степени подорвана, поскольку списки контактов, хранящиеся в этих смартфонах, скорее всего, содержат телефоны важных деловых партнеров или должностных лиц. При обнаружении DDoS-атаки целевой сервер отреагирует, заблокировав номера телефонов, из которых она исходит, что также может привести к непредсказуемым финансовым потерям и подрыву деловых отношений.

− Навязчивая реклама

  Зараженный смартфон может превратиться в приемник навязчивой рекламы. Пользователи будут получать различные рекламные объявления, каждое нажатие на которые приносит доход владельцу бот-сети. Таким способом эти люди получают огромную мошенническую прибыль от несанкционированной рекламы. При этом на рекламные объявления нажимает не пользователь смартфона, а установленный на нем вредоносный бот.

− Несанкционированный доступ к корпоративной сети

  Бот-сети, использующие смартфоны, позволяют злоумышленникам получить доступ к защищенным корпоративным сетям через зараженные сетевые устройства. Инфицированное устройство анализирует хост-компьютеры в корпоративной сети на уязвимость и сообщает результат владельцу бот-сети. Затем злоумышленники используют выявленную уязвимость для атаки на компьютеры в корпоративной сети и кражи конфиденциальной информации.

8.4 Потребление ресурсов

Владельцы бот-сетей могут вызвать резкое снижение производительности смартфонов следующими способами:

− Компоненты вируса могут быть замаскированы под графические изображения формата PNG, тогда как на самом деле это автоматизированные сценарии. После заражения вирус автоматически загружается при запуске смартфона и постоянно работает в фоновом режиме, вызывая серьезное снижение производительности операционной системы.

− Частое обращение за инструкциями к троянским серверам ведет к постоянному повреждению смартфона.

− Автоматическая загрузка спам-приложений в фоновом режиме вызывает разрядку батареи и серьезное снижение производительности за короткий период времени.

− Владельцы бот-сети постоянно рассылают SMS-спам на зараженные смартфоны, что приводит к прекращению работы смартфона и полной разрядке его батареи.

8.5 Несанкционированная передача

Некоторые вредоносные программы могут в фоновом режиме без разрешения пользователя загружать в зараженный смартфон приложения, которые затем вызывают всплывающие мошеннические сообщения, призывающие пользователя прикоснуться к экрану, что приводит к установке вредоносного ПО. Как только приложение установлено, оно тайно обращается к определенному веб-сайту, повышая его рейтинг загрузок, тем самым склоняя к загрузке вредоносных приложений новых пользователей. Таким образом бот-сеть расширяется, и злоумышленники получают еще больше прибыли.

8.6 Потеря доверия

Инфицированные бот-сетями смартфоны могут использоваться для рассылки спам-писем или участия в DDoS-атаках; такое поведение не только повышает расходы на услуги сети и потребление энергии от батареи, но и приводит к потере доверия к пользователю. Например, когда зараженный смартфон осуществляет массовую рассылку спам-сообщений или электронных писем по хранящимся в нем контактным адресам/телефонам, это подрывает доверие к отправителю (владельцу смартфона). В частности, если взломанный смартфон принадлежит определенной компании или государственному учреждению, их репутация может быть подорвана, поскольку список контактов, хранящийся в смартфоне, скорее всего, содержит телефоны важных деловых партнеров или чиновников.

9 Требования к средствам безопасности

9.1 Требования к средствам безопасности сети

9.1.1 Мониторинг сетевого трафика

Операторы должны предлагать возможность мониторинга интернет-трафика смартфона. Они могут установить механизм мониторинга трафика или таблицу, содержащую всех пользователей, и интеллектуально анализировать интернет-трафик смартфона. При обнаружении аномального трафика операторы могут немедленно направить пользователю сигнал тревоги или соответствующую информацию, а при необходимости перехватить подозрительный трафик.

9.1.2 Обнаружение вредоносного кода для мобильных устройств

Устройства защиты в сети оператора должны обнаруживать и анализировать свои приложения на отсутствие вредоносного кода. Если в приложении обнаружен вредоносный код, оператор может своевременно направить тем, кто загружает или использует приложение, сигнал тревоги или соответствующую информацию.

9.1.3 Передача зашифрованной конфиденциальной информации

Сеть оператора должна поддерживать передачу смартфонами зашифрованной информации. Если пользователь смартфона включил эту функцию, сетевые устройства оператора должны гарантировать целостность и конфиденциальность передаваемой информации, включая списки контактов, местоположение, учетные записи и пароли и т. д.

9.1.4 Использование сети-приманки

В сети оператора должна быть установлена компьютерная система, действующая как приманка для бот-сетей и вредоносных программ для смартфонов. После обнаружения бот-сети и получения ее управляющей информации оператор сможет вести наблюдение и отслеживание с целью выяснить, как лучше защитить смартфоны.

9.1.5 Защита от DDoS-атак

- Устройства защиты и серверы системы наименований доменов (DNS) в сети оператора должны иметь возможность обеспечить такую конфигурацию правил безопасности, которая препятствует подключению бот-сетей к ее контроллерам.
- В сети оператора должны присутствовать брандмауэры, системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS) и другие устройства защиты, позволяющие создать такую конфигурацию правил безопасности, при которой злонамеренный трафик будет блокироваться.
- Устройства защиты и обеспечения безопасности в сети оператора должны обеспечивать такую конфигурацию правил блокирования трафика DDoS, которая сможет блокировать трафик DDoS целевого сервера в других доменах.

9.1.6 Обнаружение бот-сетей

Устройства защиты в сети оператора должны обнаруживать мутации бот-сетей и собирать и распространять глобальный список надежных адресов протокола Интернет (IP), так чтобы можно было создать надежную базу данных IP-адресов контроллеров и хост-компьютеров бот-сетей для фильтрации вредоносного трафика, анализа действий ботов, разработки механизмов проверки IP-адресов и других методов защиты.

9.1.7 Обнаружение и удаление SMS-спама

В сети оператора должны присутствовать механизмы обнаружения и удаления SMS-спама. Когда появляется мобильный терминал, принимающий большое количество спам-сообщений, должна выполняться своевременная блокировка спама во избежание коллапса, вызванного приемом массовых спам-сообщений. При обнаружении атаки операторы должны информировать пользователей, с тем чтобы те могли принять соответствующие защитные меры.

9.1.8 Черный и белый списки

Устройства защиты в сети оператора должны обеспечивать возможность добавления вредоносных программ и веб-сайтов в черные списки. Если контроллеры бот-сети подают контролируемым ими хост-компьютерам команду на подключение к вредоносному веб-сайту или загрузку вредоносного ПО, входящего в черный список, устройства защиты должны иметь возможность своевременно блокировать эти соединения.

Аналогичным образом, устройства защиты в сети оператора должны обеспечивать и белый список. В некоторых особых случаях пользователям разрешается устанавливать соединение только с доверенными веб-сайтами и загружать надежные приложения из белого списка.

9.1.9 Способность к сотрудничеству

В целях повышения степени целостности и надежности программного обеспечения безопасности операторы должны сотрудничать с поставщиками программных продуктов для обеспечения безопасности смартфонов. Благодаря этому сотрудничеству может быть обеспечена защита от бот-сетей как со стороны сети, так и со стороны мобильного терминала.

Операторы должны также сотрудничать с государственными и административными органами. Если смартфон становится ботом, операторы должны уведомлять его владельца через административные органы. В дополнение к этому для пресечения бот-сетей, использующих смартфоны, и их вредоносного поведения операторы должны сотрудничать с государственными и административными органами в области разработки соответствующих планов действий и законодательства.

9.1.10 Гарантия идентичности

Если смартфон пользователя (а особенно смартфоны группы пользователей) взломан и начинает рассылать массовые спам-сообщения и т. д., это может привести к потере доверия со стороны получателей спама. Если зараженные смартфоны принадлежат определенным компаниям или государственным учреждениям, то ущерб может оказаться гораздо бóльшим, поскольку их списки контактов, вероятно, содержат телефоны важных деловых партнеров или государственных учреждений.

Во избежание такой потери доверия операторы должны гарантировать идентичность пользователя смартфона (в особенности групповых пользователей) с обнаружением аномальных операций, таких как массовая рассылка сообщений. Например, оператор должен обнаруживать операции групповой рассылки сообщений пользователем и, основываясь на заранее определенных правилах, информировать его посредством сообщения или временно приостанавливать операцию групповой рассылки сообщений, запрашивая подтверждение пользователя для продолжения этой операции.

9.2 Требования к средствам безопасности смартфонов

9.2.1 Хранение личной информации в зашифрованном виде

Смартфоны должны поддерживать хранилище зашифрованных списков контактов, SMS-сообщений, фотографий, записей звонков и другой PII. PII должна храниться в смартфонах с использованием методов шифрования.

9.2.2 Доступ к зашифрованной информации, позволяющей идентифицировать личность

Смартфоны должны поддерживать механизм доступа к зашифрованным спискам контактов, SMS-сообщениям, фотографиям, записям звонков и другой PII. Пользователи смартфонов должны иметь возможность устанавливать пароли, проверку отпечатков пальцев и другие средства защиты доступа к определенным видам личной информации (например, к определенным фотографиям или SMS).

9.2.3 Использование программного обеспечения безопасности

Пользователи должны установить на свои смартфоны программное обеспечение безопасности. Это поможет им обнаруживать и устранять потенциальные угрозы или уязвимости, а также принимать необходимые меры защиты в случае атаки. Если на смартфоне нет защитного программного обеспечения, он должен обеспечивать возможность напоминания пользователю о необходимости его установки. Если программное обеспечение установлено, смартфон должен обеспечивать возможность напоминать пользователю о необходимости регулярно проверять систему и обновлять программное обеспечение безопасности.

9.2.4 Предупреждение о привязке банковского счета

Если пользователь решил сохранить номера учетных записей или паролей при использовании функций мобильных платежей, то смартфон должен быть способен предупредить его о том, что хранить номера учетных записей или паролей в смартфоне не рекомендуется.

9.2.5 Мониторинг интернет-трафика в смартфонах

Программное обеспечение безопасности смартфонов должно интеллектуально анализировать использование интернет-трафика. Обнаружив аномальный трафик в течение короткого периода времени, оно должно как можно скорее заблокировать подозрительный трафик и предложить пользователю отключить сетевое соединение или прекратить просмотр любых подозрительных веб-сайтов.

9.2.6 Удаление вредоносного кода из мобильных устройств

Обнаружив вредоносный код в приложениях или вредоносных программах, смартфон должен сообщить об этом пользователю. Пользователь решит, следует ли ему удалить данное программное обеспечение и сообщить о нем в соответствующие органы.

9.2.7 Безопасное использование Wi-Fi

Для защиты PII-информации пользователя, такой как номера учетных записей и пароли, и предотвращения атак через посредника (MITM) при использовании Wi-Fi смартфоны должны обеспечивать меры, гарантирующие безопасное использование Wi-Fi. Например, когда пользователь включает Wi-Fi-соединение, смартфон может автоматически включать функцию шифрованной передачи и автоматически отключать ее, когда Wi-Fi-соединение выключено.

9.2.8 Сторонние механизмы проверки

При осуществлении пользователем смартфона мобильного платежа или работы с другим приложением, для которого требуется вход в учетную запись, смартфон должен поддерживать стороннюю проверку платежа, например распознавание голоса или использование кода проверки изображения.

9.2.9 Мониторинг потребления ресурсов

Смартфон должен быть способен контролировать производительность центрального процессора (ЦП) и энергопотребление. При аномальном расходе ресурсов ЦП или заряда батареи он должен подавать сигнал, информирующий пользователя.

Дополнение I

Вредоносные программы, подключающиеся к бот-сети

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Предисловие

Настоящее дополнение основано на кабинетном исследовании с использованием имеющихся данных, а не на первичном исследовании. Данные и аналитические отчеты получены от китайских и всемирных консультационных организаций, а также компаний, разрабатывающих антивирусное программное обеспечение. Считается, что выводы этих компаний и организаций основаны на большом количестве собранных данных и анализе больших данных.

В разных странах существуют разные культуры, обычаи, законы, нормы и правила, что приводит к разным экосистемам и экологической среде для распространения вирусов и вредоносных программ, использующих смартфоны. Например, антивирусные компании могут по собственному усмотрению переоценивать количество обнаруженных атак, основываясь на неточных определениях, и подгонять результаты анализа. Поэтому отчеты разных компаний и организаций могут демонстрировать разные статистические показатели. Однако основные выводы и тенденции, как правило, остаются неизменными.

Кроме того: 1) многие, если не большинство обнаруженных вредоносных программ обладают функциями и возможностями, которые легко могут быть использованы бот-сетями; 2) исследования тенденций в области вредоносного ПО и опыта эксплуатации смартфонов указывают на угрозу со стороны бот-сетей, использующих смартфоны, в ближайшем будущем; 3) сегодня, благодаря глобализации, некоторые региональные проблемы, связанные с вредоносными программами для мобильных устройств и бот-сетями, могут быть перенесены в другие регионы и в будущем создать еще более серьезные проблемы, поэтому необходимо быть наготове.

I.2 Введение

Быстрый рост числа смартфонов является, пожалуй, одним из величайших достижений нашего времени. Например, в Китае общее число пользователей мобильных телефонов превысило 1,3 млрд., причем более 0,68 млрд. – это пользователи смартфонов и "сетяне".

Сегодняшние смартфоны имеют минимальное количество уязвимостей, что приводит к меньшему числу вирусных инфекций. Фактически разработка смартфонов привела к появлению изделий, лишь небольшая часть которых будет взломана. Однако даже если вероятность заражения невелика, зараженный телефон может стать причиной невыносимых и необратимых потерь для пользователя, хранящего в своем смартфоне важнейшую PII, такую как номера банковских счетов, пароли, домашний адрес и фотографии близких.

Растущая популярность смартфонов привела к тому, что разработчики вирусов и вредоносных программ переориентировались с ПК на смартфоны, которые стали главной мишенью хакерских атак. Кроме того, большинство киберпреступлений, нацеленных на смартфоны, мотивированы не личным интересом и любопытством, а получением финансовой выгоды путем требования выкупа и мошенничества. За деятельностью киберпреступников стоит черная индустрия интернет-мошенничества, и это вряд ли изменится в ближайшем будущем. В дополнение к этому интернет вещей (IoT) объединяет интеллектуальные терминалы для эффективной передачи и совместного использования данных и информации. В своем недавнем исследовании аналитическая фирма Gartner [b-Gartner] прогнозирует, что в 2015 году в среде потребителей услуг "умного" дома будет использоваться более 4,9 млрд. устройств, подключенных к IoT, а в 2020 году – 25 млрд. Однако это еще больше усилит угрозу для PII пользователей, так как единственный пробел в защите/лазейка/утечка в цепочке потоков данных или разрозненная информация, собираемая из каналов IoT, могут привести к утечке PII пользователей, что создаст новые проблемы для безопасности мобильных устройств.

Следовательно, пользователям смартфонов необходимо уделять больше внимания безопасности, особенно когда речь идет о защите своей PII. Всемирная аналитическая компания *mSecurity* [b-mSecurity] сообщает, что в 2014 году инвестиции в безопасность мобильных устройств достигнут 11 млрд. долл. США и в ближайшие шесть лет будут расти в среднем на 20% в год [B-GNSM].

I.3 Макросреда в Китае

Существуют конкретные данные, подтверждающие тенденцию к экспоненциальному росту числа вредоносных программ для мобильных устройств.

В Китае, например, в последние годы популярность смартфонов быстро растет. Основываясь на исследованиях *Qihoo 360*, одной из крупнейших китайских компаний, специализирующихся на сетевой и информационной безопасности, число пользователей мобильных телефонов увеличилось с 1 млрд. в 2012 году до 1,3 млрд. в 2015 году, а число пользователей смартфонов ("сетян") за тот же период выросло с 270 млн. до 680 млн.

В течение этого периода возникло множество проблем, связанных с безопасностью. В 2012 году было выявлено 175 тыс. новых образцов мобильных вредоносных программ и зафиксирован 71 млн. случаев заражения смартфонов. В 2015 году было выявлено уже 18,7 млн. новых образцов мобильных вредоносных программ и зафиксировано 370 млн. случаев заражения смартфонов. Из-за утечки PII через бесплатный Wi-Fi и создания сценариями вредоносного ПО дополнительного трафика пользователи были вынуждены приобретать страховку от потерь, вызванных незапланированными мобильными платежами, навязчивыми телефонными звонками, утечкой PII через подержанные смартфоны или ПО социальных сетей и всевозможным спамом. Чтобы смартфон работал в здоровой и безопасной среде, необходимы защита от вирусов и вредоносного ПО, мониторинг трафика, защита PII, мониторинг скорости передачи данных по сети и мониторинг безопасности Wi-Fi. Для обеспечения лучшей защиты и безопасности смартфонов компании, специализирующиеся на программном обеспечении безопасности мобильных устройств, должны тесно сотрудничать с производителями смартфонов.

I.4 Проблемы iPhone

Платформа Apple iPhone обеспечивает повышенный уровень контроля за программным обеспечением, которое могут устанавливать пользователи, по сравнению с другими платформами, такими как Android. Компания Apple утверждает, что она гарантирует более высокий уровень безопасности [b-AppleSecurity], поскольку заинтересована в создании такой экосистемы программного обеспечения и все для этого делает. Apple постепенно продвигается к модели, в которой аппаратные средства и операционные системы тесно интегрированы, а пользователи приобретают программное обеспечение главным образом на официальном сайте App Store.

Однако имеются сообщения о появлении все большего числа вредоносных программ, заражающих устройства под управлением iOS [b-AppleThreat]. Новые исследования показывают, что наряду с быстрым ростом числа пользователей iPhone и iPhone-приложений общее восприятие безопасности iPhone ухудшается.

Код XcodeGhost (обнаруженный компанией Symantec под именем OSX.Codgost на компьютерах с Mac OS X и под именем IOS.Codgost на iOS-устройствах) представляет собой модифицированную версию среды разработки Xcode и считается вредоносным ПО. Он настраивает приложения на сбор информации об устройствах и ее передачу на C&C-серверы. Кроме того, эта троянская программа способна получать от C&C-серверов команды на осуществление фишинговых атак. Большое число приложений, созданных с помощью XcodeGhost, смогло обойти проверки безопасности и было размещено в официальном магазине приложений Apple. Это продемонстрировало, что процесс проверки не гарантирует отсутствие вредоносного ПО в App Store. В ноябре 2015 года в неофициальных версиях Xcode 7 был обнаружен новый вариант XcodeGhost, позволявший разработчикам создавать приложения для iOS 9.

Опросы показывают, что почти половина пользователей iPhone больше не считает свой телефон абсолютно безопасным. Согласно исследованиям, было взломано почти 33% смартфонов, тогда как для iPhone этот показатель составляет 23,9%.

В настоящее время телефоны Apple, в отличие от телефонов Android, лучше контролируют исполнение приложений/кодов с помощью механизма ключа разрешения разработчика. Как только в устройствах Apple обнаруживаются такие вредоносные приложения/коды, Apple может прекратить их работу сразу на всех своих устройствах, просто отвергнув ключ подписи разработчика.

Хотя iOS не является открытой платформой, у нее тоже есть свои болевые точки, а именно – навязчивые телефонные звонки и фишинг. По этой причине в июне 2016 года на Всемирной конференции разработчиков Apple (WWDC), которая состоялась в Сан-Франциско, Apple представила API-интерфейс Ident-A-Call. Он в значительной мере избавит пользователей iPhone от беспокоящих телефонных звонков и фишинга, но это также показывает, что безопасность мобильных устройств становится очень серьезной проблемой. Это уже не чисто техническая проблема – она становится также и социальной.

I.5 Примеры и некоторые тенденции нового вредоносного ПО

I.5.1 Пример 1

Новым объектом для вирусов и вредоносного ПО становится программное обеспечение социальных сетей и мобильных платежей; это происходит главным образом по причине их тесного взаимодействия и ввиду того, что каждая из этих областей становится все более важной в повседневной жизни.

Вредоносная программа *a.privacy.BankSteal.a* маскируется под известное приложение социальной сети с тем же известным логотипом, в связи с чем пользователям трудно отличить вредоносное ПО от легального. Взломав смартфон, вредоносная программа склоняет пользователя к вводу PII, такой как номера банковских карт, пароли, имена пользователей, номера удостоверений личности и телефонные номера, а затем начинает работать в фоновом режиме, перехватывая SMS-сообщения пользователя. Затем вредоносная программа отправляет собранную информацию хакерам по электронной почте. Это вредоносное ПО существенно подрывает безопасность PII и собственности пользователя.

I.5.2 Пример 2

В 2015 году во всех регионах наблюдался рост интенсивности использования смартфонов для получения банковских онлайн-услуг. Сегодня многие учреждения предлагают Android-приложение с двухфакторной аутентификацией (2FA). Это еще больше ускорило разработку мобильного вредоносного ПО [b-FinancialThreat].

Наиболее распространенный метод атаки – перехват текстовых сообщений, которые являются частью процесса 2FA, и их переадресация на C&C-сервер вредоносного ПО для использования злоумышленниками. Как обычно в случае вредоносных программам для Android, на этапе установки приложение запрашивает разрешение на получение, запись и отправку текстовых сообщений, а также некоторые другие разрешения.

В типичной системе 2FA второй фактор, обычно одноразовый пароль (OTP), передается посредством SMS по зарегистрированному номеру мобильного телефона пользователя. В целях повышения безопасности доставки OTP некоторые финансовые организации вместо SMS начали доставлять OTP посредством голосового вызова. В последнем квартале 2015 года был обнаружен новый вариант *Android.Bankosy*. Это вредоносное ПО крадет информацию из Android-устройства, обманывая системы 2FA, использующие голосовые вызовы. Его C&C-сервер может поручить зараженному смартфону переадресовку всех вызовов с использованием специального служебного кода.

Еще один распространившийся класс атак – использование автономных фальшивых банковских приложений. Они могут быть очень убедительными для пользователей, например когда вредоносная программа выглядит как легальное приложение, использующее маркер 2FA. Самым опасным аспектом вредоносных приложений этого типа является то, что на этапе установки они запрашивают у пользователя имя и пароль его учетной записи, получая всю информацию, необходимую мошеннику. Это может привести к взлому банковских счетов без использования зараженного настольного компьютера. В других случаях злоумышленники заменяют легальное установленное программное обеспечение мобильного банкинга своим собственным вредоносным ПО. Другая программа для Android, Android.Fakelogin, использует гибкие методы социальной инженерии для кражи банковских реквизитов у широкого круга пользователей. Вместо того чтобы маскироваться под конкретное приложение, Android.Fakelogin определяет, какое банковское приложение работает на пользовательском устройстве, и накладывает на интерфейс пользователя настраиваемую фальшивую страницу входа в систему. Это делается с помощью логики, размещенной в облаке на удаленном C&C-сервере, которая определяет точную фишинговую страницу для отображения. Когда пользователь пытается войти в систему через эту мошенническую страницу, его учетные данные передаются на C&C-сервер злоумышленника. Хотя вредоносное ПО нацелено на легальные приложения, доступные в Google Play, приложения, загружающие Fakelogin, в Google Play недоступны.

I.5.3 Пример 3

Одной из многих новых тенденций является то, что новые вредоносные программы все более изощренно и беспардонно шантажируют пользователей смартфонов. Например, с 2014 года все больше вредоносных программ для мобильных устройств атакуют отдельных пользователей через одноранговые (P2P) сети.

Вредоносная программа *a.rogue.SimpleLocker.a* заставляет смартфон пользователя запускать ее с наивысшим приоритетом, часто блокируя экран смартфона. За разблокирование экрана пользователь должен заплатить; в противном случае на смартфоне не смогут работать другие приложения. После оплаты вредоносное ПО устанавливает связь через интернет в фоновом режиме и позволяет удаленно разблокировать экран. Вредоносное ПО больше не прячется, а нагло присваивает себе наивысший приоритет, вымогая у пользователей выкуп. Чем больше смартфонов взломано, тем больший доход получают хакеры.

I.6 Заключение

С быстрым развитием мобильного интернета смартфоны приобретают все новые интеллектуальные и функциональные возможности. Возможно, что быстрый рост популярности смартфонов – одно из величайших достижений нашего времени, и опросы показывают, что бот-сети на базе ПК стремительно переориентируются на смартфоны. Скорость переноса вирусов и вредоносного ПО столь же ошеломляюща, как и рост популярности самих смартфонов. Поэтому работа по противодействию бот-сетям, использующим смартфоны, перспективна и полезна.

Библиография

[b-ITU-T X.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T X.1546] Рекомендация МСЭ-Т X.1546 (2014 г.), *Перечень и характеристики атрибутов вредоносного программного обеспечения*.

[b-ITU-T X-Sup.8] Рекомендации МСЭ-Т серии X − Добавление 8 (2010 г.), *МСЭ-Т X.1205 − Добавление, касающееся передовых методов противодействия угрозам бот-сетей.*

[b-AppleSecurity] Веб-страница: *Apple Claims Better Security with iOS 9, Gets Hacked before Its Release*, 13 сентября 2015 года.
<https://lifars.com/2015/09/hacker-cracks-ios-9-with-a-jailbreak-before-its-public-release/>

[b-AppleThreat] O'Brien, Dick (2016), *The Apple threat landscape*, Symantec Symantec Security Response, Version 1.02, February 11, 2016.

[b-FinancialThreat] Candid, West (2015), *Financial* threats, Symantec Security Response, Version 1.0, March 22, 2016.

[b-Gartner] Пресс-релиз Gartner, 11 ноября.
<http://www.gartner.com/newsroom/id/2905717>

[b-GNSM] *Global Network Security Market 2015-019.*

[b-mSecurity] Прогноз рынка средств безопасности для мобильных устройств (mSecurity) на 2014–2024 годы.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.