Защищая корпоративный периметр

Исследование Positive Technologies: как хакеры скрывают следы атак на государственные и образовательные учреждения

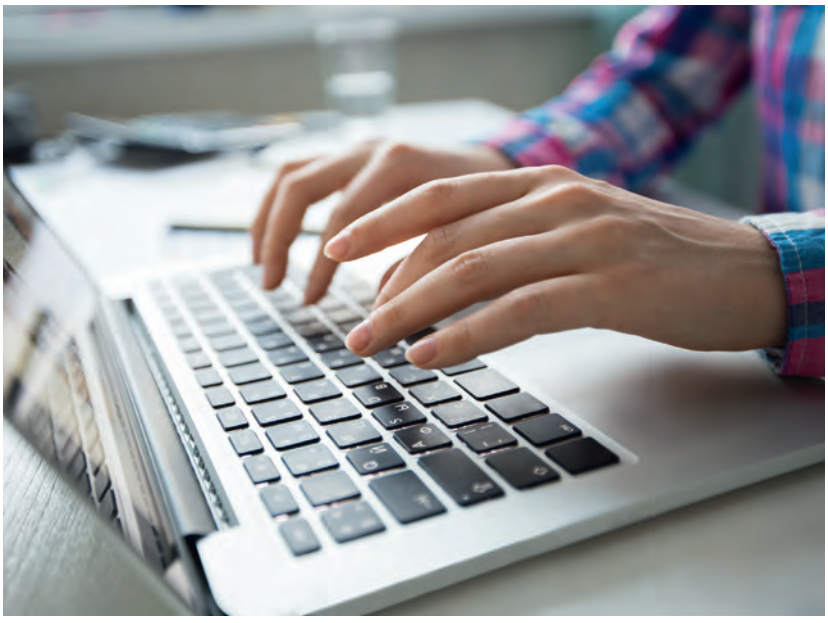
Минувшие два года в условиях пандемии характеризуются возрастанием угроз кибербезопасности. Рост числа дистанционных подключений различных гаджетов, цифровизация бизнес-процессов увеличивают угрозу кибератак. В зоне особого внимания – крупные предприятия, где задействованы большое количество автоматизированного оборудования со множеством технологических операций и многочисленный персонал.

Такую активность можно связать с тем, что почти все предприятия начали больше работать в онлайн-режимах. Организация удаленной работы при недостаточном обеспечении защиты может создавать серьезную угрозу проникновения.

Эксперты Positive Technologies проанализировали наиболее известные за последние 10 лет семейства руткитов – программ, позволяющих скрыть в системе присутствие вредоносного программного обеспечения или следы пребывания злоумышленников. Исследование показало, что 77 % руткитов используются киберпреступниками для шпионажа.

Руткиты – не самое распространенное вредоносное ПО. Случаи обнаружения руткитов, как правило, отсылают к громким атакам с резонансными последствиями – зачастую данные утилиты входят в состав многофункционального вредоносного ПО, которое перехватывает сетевой трафик, шпионит за пользователями, похищает сведения для аутентификации или использует ресурсы жертв для проведения DDoS-атак. Наиболее известный случай применения руткита в атаках – кампания по распространению вредоносного ПО Stuxnet, главной целью которой была приостановка развития ядерной программы Ирана.

Аналитики Positive Technologies провели масштабное исследование руткитов, используемых злоумышленниками за последние десять лет – начиная с 2011 года. Согласно полученным данным, в 44 % случаев злоумышленники использовали руткиты в атаках на госучреждения. Чуть реже (38 % случаев) эти вредоносы применялись для атак на исследовательские институты. Эксперты связывают выбор этих целей с основным мотивом киберпреступников – получением данных. Так, большую ценность для злоумышленников представляет информация, которую обрабатывают эти организации. В топ-5 наиболее атакуемых посредством руткитов отраслей по итогам исследования также

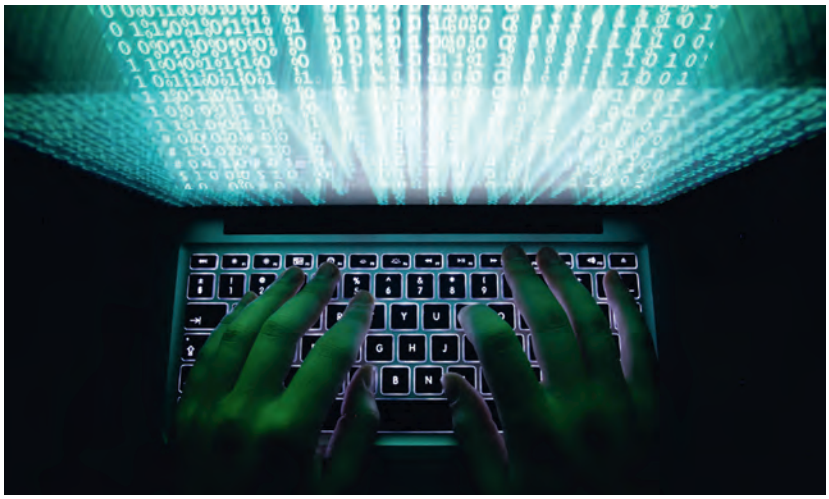


вошли телеком (25 %), промышленность (19 %) и финансовые организации (19 %). Помимо этого, более половины руткитов (56 %) используются хакерами в атаках на частных лиц. Главным образом речь о таргетированных атаках в рамках кампаний по кибершпионажу в отношении высокопоставленных чиновников, дипломатов и сотрудников целевых организаций.

Руткиты, особенно работающие в режиме ядра, очень сложны в разработке, поэтому их используют либо высококвалифицированные APT-группировки, которые обладают навыками разработки подобного инструмента, либо группы, чьи финансовые возможности позволяют купить руткиты на теневом рынке. Основная цель злоумышленников такого уровня – кибершпионаж и получение данных. Это могут быть как финансово мотивированные преступники, которые похищают крупные суммы денег, так и группировки, добывающие информацию и совершающие разрушительные действия в инфраструктуре жертвы в интересах заказчиков.

Как показал анализ, исследованные семейства руткитов в 77 % случаев использовались злоумышленниками для получения данных, примерно в трети случаев (31 %) – для извлечения финансовой выгоды, и лишь в 15 % атак эксперты отметили мотив эксплуатации инфраструктуры компании-жертвы для проведения последующих атак.

Согласно отчету Positive Technologies, на теневых форумах в основном преобладают объявления о продаже руткитов пользовательского уровня – их обычно используют в массовых атаках. По оценкам экспертов компании, стоимость готового руткита варьируется от 45 до 100 000 долл. США и зависит от режима



работы, целевой ОС, условий использования (например, вредонос можно взять в аренду на месяц) и дополнительных функций (чаще всего запрашивают получение удаленного доступа и сокрытие файлов, процессов и сетевой активности). В некоторых случаях разработчики предлагают доработку руткита под нужды заказчика и оказывают сервисное сопровождение. Стоит отметить, что в 67 % объявлений фигурировало требование о том, что руткит должен быть «заточен» под Windows. Это коррелирует с результатами исследования: доля таких образцов в выборке вредоносов, изученных специалистами Positive Technologies, также превалирует, составляя 69 %.

Несмотря на сложности разработки этих зловредов, каждый год мы отмечаем появление новых версий руткитов, чей механизм работы отличается от уже известных вредоносов. Это говорит о том, что киберпреступники продолжают развивать инструменты, позволяющие маскировать вредоносную активность, и постоянно придумывают новые техники обхода средств защиты – появляется новая версия Windows, и сразу же разработчики вредоносов создают руткиты, ориентированные под нее. Мы ожидаем, что руткиты продолжат использовать хорошо подготовленные APT-группировки, а значит, речь идет уже не просто о компрометации данных и извлечении финансовой выгоды, а о сокрытии сложных целенаправленных атак, результатом которых может быть реализация недопустимых для организаций событий – от вывода из строя объектов КИИ, таких как атомные станции, ТЭЦ и электросети, до техногенных катастроф, вызванных авариями на промышленных предприятиях, и случаев политического шпионажа.

Чтобы обезопасить свою компанию от атак с использованием руткитов, специалисты Positive Technologies рекомендуют применять средства обнаружения вредоносной активности на конечных узлах и решения типа PT Sandbox, которые позволяют выявить вредоносную программу как на этапе установки, так и в процессе работы. Обнаружить руткиты также поможет сканер руткитов, проверка целостности системы и анализ сетевого трафика на предмет аномалий.

Алексей Вишняков,
руководитель отдела обнаружения вредоносного ПО
Positive Technologies

Яна Юракова,
аналитик Positive Technologies

Москва