Аннотация – в документе представлен анализ публично известных частных компаний, участвующих в наступательных кибер-операциях против национальных государств. Анализ включает в себя различные аспекты инвентаризации, включая характер включённых в список компаний, типы предлагаемых ими возможностей и геополитические последствия их услуг.

Предоставленная выдержка отличается высоким качеством и объединяет общедоступную информацию без раскрытия конфиденциальных данных. Он служит ценным ресурсом для специалистов в области безопасности, предлагая представление об условиях участия частного сектора в наступательных кибер-операциях.

I. Что представляет собой Группа EQUATION?

The Equation Group классифицируется как продвинутая постоянная угроза (APT) и известна своей изощренной деятельностью по кибершпионаж с активностью как минимум с 2001 года и сложными и высокоразвитыми вредоносными инструментами и технологиями. Группа участвовала в многочисленных кибер-операциях, нацеленных на широкий спектр секторов и стран, включая правительственные, военные, телекоммуникационные, аэрокосмические, энергетические, ядерные исследования и финансовые учреждения

II. EQUATION и технологии

A. Кибер-возможности

- **Инструменты удалённого доступа и платформы вредоносных программ**: Equation использовала множество инструментов удалённого доступа и разработала несколько платформ вредоносных программ высокой сложности, таких как EquationDrug, DoubleFantasy, Equestre (то же, что EquationDrug), TripleFantasy, GrayFish, Fanny и EquationLaser. Эти инструменты предназначены для шпионажа и имеют механизмы самоуничтожения, позволяющие уменьшить количество улик.
- **Перепрограммирование встроенного ПО**: Одним из самых передовых методов, используемых Equation, является возможность перепрограммирования встроенного ПО жёсткого диска. Эта возможность позволяет группе оставаться в заражённых системах необнаруживаемой и эффективно делает их операции невидимыми и неуязвимыми.
- **Шифрование и обфускация**: Equation часто использовала схемы шифрования, включая RC5, RC6, RC4, криптографические функции AES и различные хэш-функции, для защиты своих вредоносных программ и коммуникаций. Такой уровень шифрования и стратегии, используемые для маскировки её деятельности, свидетельствуют о передовых возможностях группы.
- **Использование уязвимостей нулевого дня**: Группа имеет доступ к эксплойтам нулевого дня и использовала их. Например, Equation использовала два эксплойта нулевого дня в Fanny до того, как они были интегрированы в Stuxnet, что указывает на доступ к этим уязвимостям раньше других известных групп, совершавших кибератаки.
- **Инструменты разведки на базе USB**: для получения информации об устройствах, которые не подключены к Интернету, Equation разработала вредоносную программу для разведки на основе USB-накопителей. Эта способность важна для проникновения на охраняемые военные объекты, разведывательные организации и ядерные объекты.
- **Фреймворки для эксплойтов и постэксплуатационные** инструменты: Equation использовала различные фреймворки эксплойтов и инструменты для последующей эксплуатации, такие как DanderSpritz, который представляет собой полнофункциональный фреймворк, используемый после эксплойта устройства и содержит широкий спектр модулей для сохранения, разведки, бокового перемещения и обхода антивирусных систем.
- **Цепочка эксплойтов брандмауэра**: Equation разработала почти полный набор эксплойтов, предназначенный для основных производителей брандмауэров. Этот комплект включает в себя эксплойты, такие как EXTRABACON (CVE-2016–6366) для получения доступа к брандмауэрам Cisco ASA и PIX, и EPICBANANA (CVE-2016–6367) для установки командного и управляющего шелл-кода.

B. Вредоносное ПО Equation

- **EquationDrug**: сложная вредоносная платформа, предоставляющая группе полнофункциональную платформу для шпионажа.
- **DoubleFantasy**: вредоносное ПО в стиле валидатора, используемое для подтверждения того,

что цель представляет интерес, а затем для развёртывания следующего вредоносного ПО.

- **Fanny**: Червь, использующий два эксплойта нулевого дня для отображения сетей с воздушным зазором через USB-накопители.
- **GrayFish**: Платформа, которая полностью размещается в реестре, шифруя свою полезную нагрузку и сохраняя её в виртуальной файловой системе.

Одним из самых мощных инструментов в их арсенале является модуль, известный только под загадочным названием “nls_933w.dll”, который позволяет им перепрограммировать встроенное ПО жёсткого диска более чем дюжины различных марок жёстких дисков. Эта возможность является уникальным техническим достижением группы.

C. Инструменты удалённого доступа

Equation использовала несколько инструментов удалённого доступа (RATs) и известна использованием эксплойтов нулевого дня. Эти инструменты способны перезаписывать встроенное программное обеспечение дисковода, ещё раз демонстрируя расширенные возможности группы:

- **UnitedRake (UR)**: RAT-инструмент, который может быть нацелен на компьютеры с Windows. Это расширяемый и модульный фреймворк, снабжённый множеством плагинов, которые выполняют различные функции сбора информации.
- **Double Feature**: Инструмент после эксплуатации регистрирует использование других вредоносных программ на заражённом компьютере, предоставляя уникальный источник знаний, относящихся к инструментам Equation.
- **EquationLaser, EquationDrug, DoubleFantasy, Equestre (то же, что EquationDrug), TripleFantasy, GrayFish, Fanny и EquationLaser**: пользовательские платформы атак, трояны, черви и бэкдоры, используемые Equation.

III. Взаимосвязь между группой Equation и АНБ

Группа Equation подозревается в том, что она связана с подразделением АНБ по специализированным операциям доступа (Tailored Access Operations, TAO). На эту связь указывают несколько факторов:

A. Сходства между Equation и АНБ

- **Сложность и ресурсы**: Equation известна своими высокоразвитыми возможностями, включая разработку и использование сложных вредоносных программ и эксплойтов нулевого дня. Операции группы, которые охватывают десятилетия и нацелены на широкий спектр секторов по всему миру, указывают на уровень ресурсов и опыта, соответствующий такой спонсируемой государством организации, как АНБ.
- **Сходства с инструментами и методами АНБ**: Анализ вредоносных программ и эксплойтов Equation выявляет значительное сходство с теми, которые, как известно, используются АНБ. Например, использование определённых алгоритмов шифрования (RC5, RC6, RC4, AES) и методов обфускации отражает те, которые задокументированы в операциях АНБ. Кроме того, часы работы вредоносного ПО и нацеленность на конкретные страны соответствуют интересам США, что ещё раз наводит на мысль о связи с АНБ.
- **Утечка Shadow Brokers**: В 2016 году группа, известная как Shadow Brokers, обнародовала множество кибер-инструментов и эксплойтов, которые, по их утверждению, были украдены у Equation. Анализ этих инструментов показал, что они использовали уязвимости в программном и аппаратном обеспечении весьма сложными и ранее неизвестными способами, что предполагает участие организации с обширными возможностями ведения кибервойны, такой как АНБ.
- **Документы Сноудена**: Документы предоставили косвенные доказательства связи Equation с АНБ. Определённые кодовые имена и оперативные данные, обнаруженные в документах Сноудена, совпадают с теми, которые связаны с деятельностью Equation, что укрепляет уверенность в том, что группа действует под эгидой АНБ.
- **Общие эксплойты нулевого дня**: Equation имела доступ к эксплойтам нулевого дня до того, как они были использованы в других известных вредоносных программах, связанных с АНБ, таких как Stuxnet и Flame, что Equation либо является частью АНБ, либо тесно сотрудничает с ним, обмениваясь инструментами и эксплойтами для кибер-операций.
- **Экспертный анализ и атрибуция**: Эксперты и исследователи по кибербезопасности, в том числе из "Лаборатории Касперского", указали на техническую сложность, схемы таргетинга и операционную безопасность Equation как на признаки спонсируемого государством субъекта, цели которого совпадают с целями АНБ. Хотя прямое установление авторства является сложной задачей в киберпространстве, накопленные доказательства и консенсус экспертов сильно склоняются к тому, что Equation является частью АНБ или аффилирована с ним.

B. Различия между Equation и АНБ

В то время как Equation в первую очередь сосредоточена на кибершпионаже и создании и развёртывании передовых вредоносных программ, у АНБ есть более широкая миссия, которая включает как сбор разведданных, так и операции по обеспечению национальной безопасности. Деятельность АНБ охватывает широкий спектр операций, включая сигнальную разведку, кибербезопасность и глобальный

мониторинг, с целью сбора и анализа данных, имеющих отношение к национальной безопасности.

АНБ действует по всему миру и участвует в различных видах разведывательной деятельности, которые включают кибер-операции, но не ограничиваются ими. Она структурирована для поддержки более широких разведывательных и оборонных операций США, в то время как Equation специально ориентирована на сложный кибершпионаж.

C. Миссия Equation и миссия АНБ

Миссия Equation заключается в проведении кибершпионажа с целью сбора разведданных, часто путём развёртывания вредоносных программ, которые могут проникать в целевые системы и сохраняться в них незамеченными. Их операции характеризуются использованием эксплойтов нулевого дня, сложных вредоносных программ и методов, предназначенных для взлома важных объектов и сохранения их скрытности.

Напротив, миссия АНБ является более всеобъемлющей и включает в себя сбор и обработку глобальных разведывательных сигналов для принятия решений в области национальной обороны и внешней политики США. Деятельность АНБ не ограничивается кибер-операциями; она также включает широкий спектр продуктов и услуг для радиотехнической разведки и обеспечения инфобезопасности, предназначенных для защиты информационных систем США и получения иностранной радиотехнической разведывательной информации

D. Центр информационных операций Центрального разведывательного управления (ЦРУ)

Центр информационных операций Центрального разведывательного управления (IOC) играет решающую роль в расширенной миссии агентства, которая теперь включает тайные военизированные операции наряду с традиционной деятельностью по сбору разведданных. IOC, одно из крупнейших подразделений ЦРУ, переключило своё внимание с борьбы с терроризмом на наступательные кибер-операции, отражая меняющийся характер глобальных угроз и растущее значение кибервойн для национальной безопасности.

Фундамент IOC как центра цифровых и кибер-операций агентства был ещё более укреплён с созданием Директората цифровых инноваций (DDI) в 2015 году. Это новое управление, первое новое управление за пятьдесят лет, было создано для модернизации ИТ-систем ЦРУ. Он объединил ИТ-отдел шпионского агентства, кибер-возможности и разведывательные усилия с открытым исходным кодом под одной крышей, стремясь предоставить аналитикам ЦРУ более совершенные ИТ-инструменты для традиционной шпионской работы.

Создание DDI и акцент на роли IOC в кибер-операциях подчёркивают признание ЦРУ цифровой сферы в качестве важнейшего поля боя. Усилия агентства по интеграции цифровых и кибернетических возможностей в свои операции отражают более широкую тенденцию разведывательного сообщества США адаптироваться к вызовам, создаваемым цифровой эпохой, включая киберугрозы, электронное наблюдение и информационную войну

E. Группа инженерных разработок ЦРУ (EDG)

Группе инженерных разработок ЦРУ (EDG) поручено разрабатывать, тестировать и обеспечивать оперативную поддержку всех бэкдоров, эксплойтов и вредоносных полезных нагрузок, используемых ЦРУ в кибер-операциях. Эта группа играет решающую роль в создании инструментов и техник, необходимых для ведения кибершпионажа и кибервойны.

В обязанности EDG входит обеспечение того, чтобы ЦРУ поддерживало передовые возможности по проникновению в системы и сети противника, используя уязвимости в программном и аппаратном обеспечении для сбора разведданных или достижения других оперативных целей.

F. Технические аспекты кибер-операций ЦРУ (TAC)

Кибер-операции ЦРУ включают в себя сложные инструменты и методы сбора разведданных из систем и сетей противника. Это включает в себя использование передовых технологий в кибершпионаже, которые поддерживаются техническим опытом агентства.

Сотрудники ЦРУ по кибербезопасности отвечают за защиту данных и систем агентства от угроз. Они используют сложные инструменты и знания в области информационных технологий (ИТ) ЦРУ для мониторинга, оценки и управления ИТ-рисками. Это включает в себя выявление текущих угроз, снижение уровня уязвимости и прогнозирование будущих вызовов.

Отдел оперативной поддержки (OSB) ЦРУ, входящий в состав подразделения кибер-разведки, специализируется на операциях с физическим доступом, что указывает на техническую возможность разрабатывать инструменты для кибератак миссий в кратчайшие сроки, что подчёркивает техническую гибкость в кибер-операциях ЦРУ

G. TAC и EQGRP

Wikileaks даёт взгляд на оперативные проблемы, с которыми сталкиваются национальные разведывательные агентства после раскрытия их киберпотенциалов, подчёркивая постоянную необходимость повышения уровня безопасности и стратегических корректировок в кибер-операциях.

- **Совместные усилия и общие возможности**: EQGRP — это не единая организация, а собирательный термин организации под управлением TAO АНБ и IOC ЦРУ, что подчёркивает совместный характер кибер-операций между этими двумя ключевыми разведывательными структурами США.
- **Совместная разработка и авторство**: Обсуждение указывает на то, что некоторые части кибер-имплантатов, связанных с EQGRP, были созданы в соавторстве как ЦРУ, так и АНБ. Это совместное

авторство подчёркивает комплексный подход к разработке кибер-инструментов и стратегий.

- **Различия в операционных процессах**: между IOC ЦРУ и АНБ ТАО были заметные различия в процессах или их отсутствии для повторного использования кибернетических возможностей. Эти различия потенциально могут повлиять на эффективность и безопасность кибер-операций.
- **Результаты**: Утечка информации и последующее публичное разоблачение этой деятельности привели к серьёзному самоанализу в этих агентствах. Обсуждение отражает большой интерес к извлечению информации из инцидента для повышения безопасности кибер-операций.
- **Важность высококачественной информации об угрозах**: Обсуждение также подчёркивает ценность высококачественной информации об угрозах, о чем свидетельствует отчёт Касперского, который сыграл решающую роль в раскрытии этих действий. Ведомства признают необходимость понимания и смягчения последствий таких разведывательных данных для национальной безопасности.

H. Размышления

- **Схожий характер кибер-операций США**: это подчёркивает, что кибер-операции США не являются прерогативой какого-либо одного агентства. Вместо этого они предполагают сотрудничество между различными разведывательными агентствами, включая АНБ и ЦРУ. Такой совместный подход типичен для сложных кибер-операций, требующих широкого спектра навыков и ресурсов, которыми ни одно ведомство не может эффективно управлять в одиночку.
- **Роль IOC ЦРУ**: Центр информационных операций ЦРУ (IOC) выделяется как важный участник деятельности, приписываемой the Equation. Участие ЦРУ предполагает, что операции Equation имеют более широкую основу в разведывательном сообществе США, чем считалось ранее.
- **Неверная атрибуция**: проблемы и потенциальные неточности, связанные с приписыванием киберактивности конкретным группам или агентствам из-за секретного характера разведывательной деятельности и сложных технических особенностей кибервойны в т.ч. точное определение ответственности чрезвычайно сложно. Следовательно, существует тенденция чрезмерно упрощать ситуацию, приписывая все передовые кибер-операции АНБ как одному из ведомств, что безусловно не отменяет роли последнего.
- **Общественное восприятие и упрощение СМИ**: Критика СМИ и общественного дискурса часто сосредоточена на их тенденции чрезмерно упрощать повествование о кибер-операциях, приписывая их исключительно АНБ. Это чрезмерное упрощение не учитывает сложную реальность межведомственного сотрудничества и распределённый характер кибератак и возможностей ведения боевых действий.
- **Важность более широкого взгляда**: это требует более глубокого понимания того, как правительство США проводит кибер-операции. Признание участия различных агентств, помимо АНБ, важно для полного понимания возможностей и стратегий США в киберпространстве.

IV. «Вместо заключения»

- **Идентификация группы Equation**: Группа Equation идентифицирована как очень сложная и продвинутая постоянная угроза, в первую очередь связанная с подразделением специализированных операций доступа (ТАО) АНБ. Эта группа активно занималась кибершпионажем и кибервойной, используя сложные инструменты и методы для проникновения в широкий круг целей по миру.
- **Последствия утечек**: Утечки Shadow Brokers в 2016 году, раскрыли важные детали об операциях Equation, включая использование сложных инструментов, таких как Bvp47. Эти утечки подтвердили связь группы с АНБ и выявили широкий охват их кибер-операций, затронувших более 287 целей в 45 странах.
- **Техническая сложность**: Инструменты Equation, такие как Bvp47, продемонстрировали расширенные возможности при сетевых атаках, оснащённых уязвимостями 0day. Их операции характеризовались высокой степенью скрытности и технической изощрённости, что делало их доминирующей силой в противостояниях в киберпространстве на национальном уровне.
- **Глобальное воздействие и жертвы**: Глобальное воздействие деятельности Equation было огромным, жертвы были в разных странах, что указывает на стратегический и широкомасштабный характер их кибер-операций. Это включало использование систем жертв в качестве переходных серверов для дальнейших атак, что подчёркивало стратегическую глубину их операций.