Компания ООО «НПП «ИТБ»

КСЗИ «Панцирь+».
Комплексная система защиты от целевых атак

Страница продукта размещена по ссылке: http://npp-itb.ru/products/armourp

Санкт-Петербург, 2017

Решаемая проблема – реализация эффективной защиты от целевых (таргетированных) атак

Особенность целевых атак (APT) заключается в том, что злоумышленников интересует конкретная компания в различных отраслях экономики или государственная организация. Это отличает данную угрозу от массовых хакерских атак – когда одновременно атакуется большое число целей и наименее защищенные пользователи становятся жертвой. В данном случае злоумышленники изучают информационные системы конкретного атакуемого объекта, вредоносное ПО, если оно используется при реализации атаки, специально **разрабатывается** для конкретной целевой атаки, **чтобы штатные средства защиты**, изучаемые злоумышленниками, **не смогли обнаружить** ее реализацию. **Анализируется** также перед реализацией **возможность обнаружения атаки различными средствами детектирования**, в частности, поведенческими анализаторами. В частности при реализации атаки могут использоваться уязвимости нулевого дня в системном и прикладном ПО. Отличием целевых атак является и то, что подобную атаку могут осуществлять как внешние нарушители (хакеры), так и внутренние – сотрудники предприятия (инсайдеры), т.е. защита должна реализовываться в комплексе.

Основная цель атаки класса APT — кража конфиденциальной информации, которую впоследствии можно использовать для получения геополитического преимущества или продажи заинтересованным лицам, либо нарушение доступа к обрабатываемой информации.

Это атаки, наносящие сегодня максимальный ущерб по всему миру, например, ущерб финансовых организаций от целевых атак в России в 2016 году вырос почти на 300% и составил 2,5 млрд. рублей и продолжает рост, атаки же на критически важные инфраструктурные объекты уже могут иметь куда более серьезные – социальные последствия. Отметим, что стремительный рост числа подобный атак косвенно характеризует и реальную эффективность существующей защиты от подобных атак.

Принципиальным отличием целевой атаки, с точки зрения защиты от нее корпоративных ИС, является невозможность ее детектирования, как собственно процесса реализации атаки, так и используемых при осуществлении атаки вредоносных компонентов!

Резюме проекта

Используются

Антивирусная защита, обнаружение поведенческих аномалий, вторжений и т.д., основанные на детектировании вирусов и потенциально опасных событий. СЗИ НСД реализуют разграничение прав доступа между пользователями, не пригодны для защиты от целевых атак

Реализовано

Инновационная технология защиты, основанная на реализации контроля доступа субъектов к объектам, не требующего детектирования вирусов, уязвимостей и иных потенциально опасных событий, что позволяет решать задачу защиты от целевых атак в общем виде

Состояние разработки

КСЗИ «Панцирь+» может использоваться совместно с ОС семейства Microsoft Windows, начиная от Windows XP, и заканчивая Windows Server 2016, может использоваться для защиты рабочих станций, серверов, терминальных серверов, средств виртуализации Hyper-V, включая защиту и гостевых машин, и гипервизора.

1. Наличие апробированных технологических решений
2. Внедрение 8 запатентованных технических решений
3. Создана и поставляется КСЗИ «Панцирь+»

На практике сегодня защита от целевых атак реализуется различными средствами детектирования, как правило, по данным Gartner, это анализ сетевого трафика, поведенческий анализ на конечных точках (направленных на защиту от массовых атак – предотвращение эпидемий), а также применением «песочницы», что имеет смысл для защиты личных компьютеров!

Технология защиты

1. Вычислительное средство – объект защиты, может быть охарактеризовано иерархией реализуемых в нем ролей:
- роль загрузки системы (BIOS, загрузчик ОС);
- роль «система» (процесс System, системные драйверы, службы, процессы и библиотеки);
- функциональная роль объекта защиты (рабочая станция, сервер, терминальный сервер, виртуальная машина и гипервизор и т.д.);
- роль системного администрирования объекта (системный администратор и средства администрирования);
- роль защиты объекта (администратор безопасности, средства защиты и их администрирования);
- роли пользователей (интерактивные пользователи и приложения).

2. Каждая роль в общем случае характеризуется необходимым и достаточным для нее набором субъектов доступа (пользователь, процесс) и соответствующим для роли необходимым и достаточным набором объектов доступа (ресурсов).

3. Реализация технологии защиты в общем случае состоит в решении следующих задач:
- локализация режимов обработки данных в рамках соответствующих ролей - по пользователям, процессам, объектам доступа – в рамках каждой роли должны использоваться только необходимые для нее субъекты и объекты доступа, при условии предотвращения несанкционированной возможности изменения их наборов и модификации;
- изоляция режимов обработки данных в рамках различных ролей одного и различных уровней иерархии – для каждой роли должны предоставляться только необходимые и достаточные для ее реализации возможности и способы взаимодействия с другими ролями, при условии предотвращения несанкционированной возможности их изменения и модификации.

КСЗИ «Панцирь+» реализует иерархическую ролевую модель доступа к ресурсам.

Описание продукта

КСЗИ «Панцирь+» это сетевая система защиты, позволяющая в комплексе решать наиболее актуальные задачи защиты информации от внешних и от внутренних угроз, в том числе и от целевых атак.

1. Защита от внутренних угроз (от инсайдерских атак):
- от атак со стороны интерактивных пользователей, санкционированно обрабатывающих данные в информационной системе;
- от атак со стороны привилегированных пользователей (администраторов), решающих те или иные задачи администрирования в информационной системе.

2. Защита от внешних угроз (хакерских атак), в том числе, защита от вирусных атак, включая вирусы вымогатели, защита от фишинговых атак, от атак на уязвимости ОС и приложений, от атак на привилегированные учетные записи, включая атаки на учетные записи администраторов, и т.д.

Задача защиты от целевых атак – эта самая актуальная сегодня задача, так или иначе решаемая всеми ведущими вендорами в различных странах, например, это продукты Check Point SandBlast, Fortinet Advanced Threat Protection, Palo Alto Networks WildFire, Proofpoint Targeted Attack Protection, FireEye Threat Intelligence, Kaspersky Anti Targeted Attack Platform, InfoWatch Targeted Attack Detector и т.д., которые основаны на решении различных задач детектирования, что позволяет их рассматривать, в качестве средств защиты от массовых, а не от целевых атак (их задача – предотвращений эпидемий).

Ключевое отличие КСЗИ "Панцирь+" – это решение, позволяющее реализовывать эффективную защиту от целевых атак, причем в общем виде – реализацией разграничительной/разделительной политики доступа субъектов к объектам – без необходимости детектирования чего-либо. Естественно, что с тем же успехом КСЗИ "Панцирь+« может использоваться и для защиты от массовых атак.

Дополнительным преимуществом КСЗИ "Панцирь+" является наличие сертификата ФСТЭК России, причем все механизмы защиты из состава КСЗИ сертифицированы и могут легитимно использоваться в соответствующих информационных системах, требующих применения сертифицированных средств защиты информации.

Конкурентный анализ

Средства, используемые сегодня на практике для защиты от целевых атак	Check Point SandBlast, Fortinet Advanced Threat Protection, Palo Alto Networks WildFire, Proofpoint Targeted Attack Protection, FireEye Threat Intelligence, Kaspersky Anti Targeted Attack Platform, InfoWatch Targeted Attack Detector и т.д.	Защита от целевых атак реализуется различными средствами детектирования (кода, поведения и т.д.), что эффективно для защиты от массовых атак – для противодействию эпидемий, уже после того, как выявлен факт и идентифицированы признаки успешно реализованной целевой атаки.
Сертифицированные СЗИ НСД	Dallas Lock, Secret Net и др.	В принципе не предназначены для реализации защиты от целевых атак, позволяют выполнять требования регулятора в области ИБ.
Комплексная система защиты информации	КСЗИ «Панцирь+»	Эффективная защита от целевых атак реализуется в общем виде, без использования каких-либо средств детектирования основанных на выявлении сигнатур, как СЗИ НСД выподняются требования регулятора в области ИБ.

Спасибо за внимание!

Презентация КСЗИ «Панцирь+» размещена по ссылке:
http://npp-itb.ru/images/docs/alldocs/present.pdf

А.Ю. Щеглов
E-mail: info@npp-itb.spb.ru,
http://www.npp-itb.ru