Понимание кибер-атак

Часть I. Cyber-Kill Chain.

Adaptive Defense

pandasecurity.com/intelligence-platform/

Содержание

1. Введение.

Меняющийся пейзаж угроз, их частота появления, сложность и целевой характер атак требует эволюции действующих правил безопасности с переходом к сочетанию технологий **предотвращения, обнаружения и реагирования на кибер-атаки**.

Большинство организаций имеют средства для обнаружения известных атак, хотя иногда могут встречаться компании и без таких решений. Самое сложное - это остановить неизвестные атаки, которые специально созданы с целью обхода имеющейся защиты за счет изменения сигнатур и шаблонов поведения.

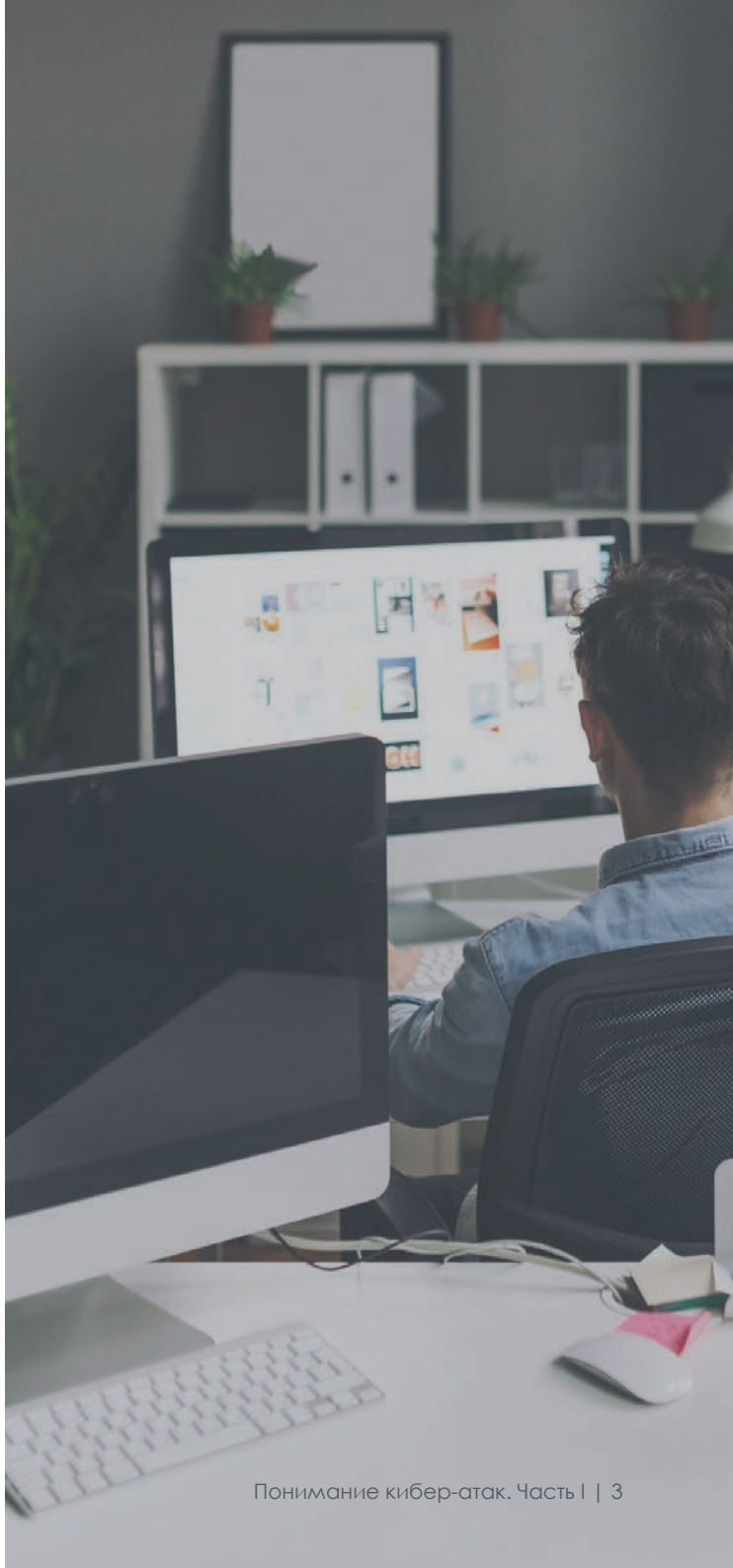
Многие организации уже вложили серьезные средства в создание собственной команды по охоте за угрозами и/или в передачу сервис-провайдерам критически важной задачи постоянного улучшения своих техник защиты и поиска лучших инструментов и способов обеспечения безопасности своей интеллектуальной собственности и цифровых активов.

Понимание того, как осуществляются кибер-атаки, и сопоставление стратегии защиты предприятия с их жизненным циклом показывают, как можно обнаруживать, останавливать и срывать эти атаки, восстанавливаться после них и где должны быть усилены операции по обеспечению безопасности.

Данный отчет помогает специалистам по безопасности понять известную модель жизненного цикла кибер-атак под названием Cyber-Kill Chain (CKC) и ее расширение на всю сеть, а также разобраться в том, как Panda Adaptive Defense покрывает весь жизненный цикл на уровне конечной точки.

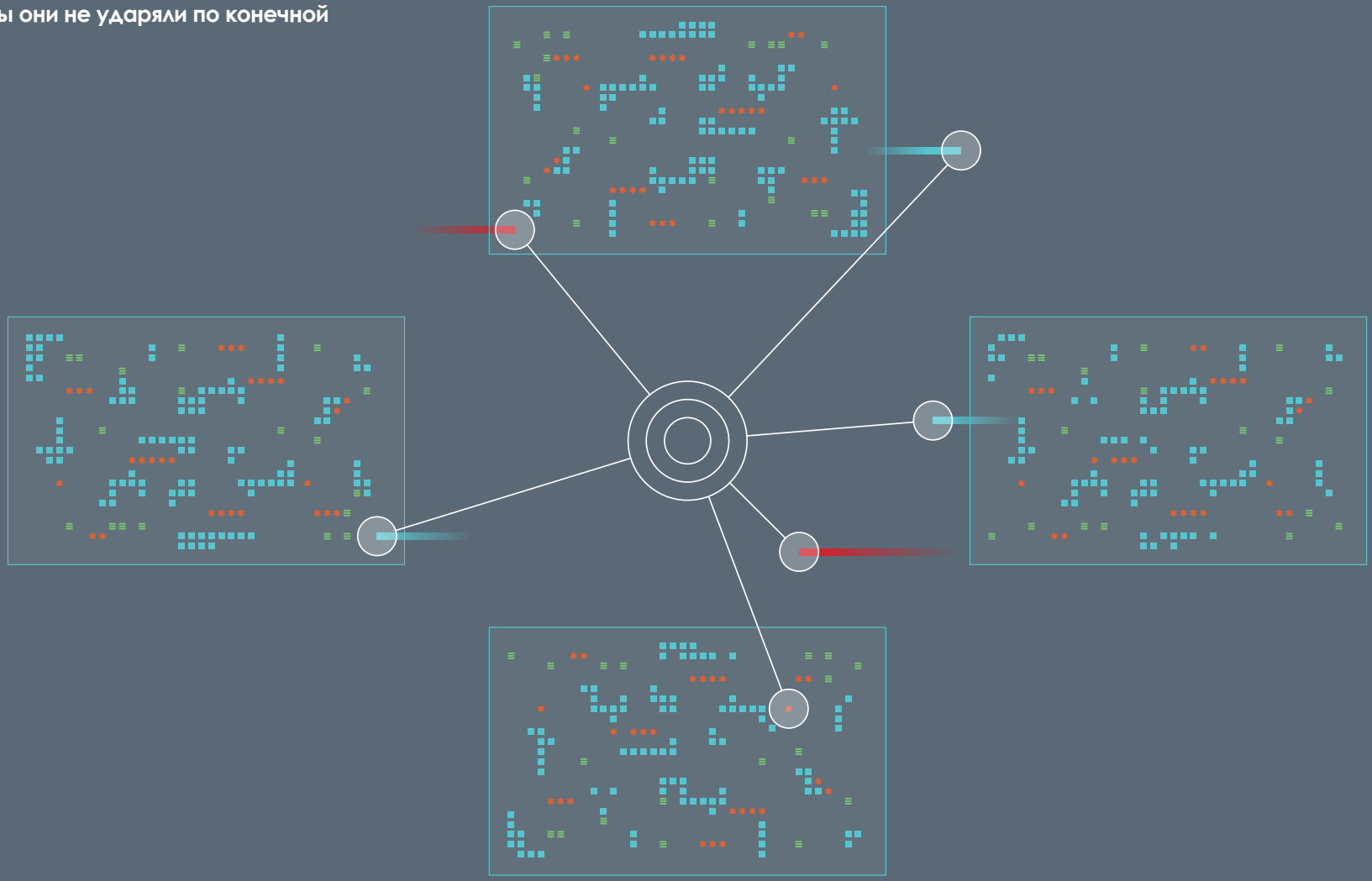
Cyber-Kill Chain, и ее расширение на всю сеть, - это отличный инструмент для понимания того, как компании могут значительно усилить обороноспособность своего окружения, ловя и останавливая угрозы на каждой фазе жизненного цикла атаки. Kill Chain учит нас, что в то время как хакеры для достижения успеха должны пройти все этапы процесса, нам "всего" лишь необходимо остановить атаку на любом этапе процесса, чтобы ее сорвать.

Учтите, что большинство ценных активов компании (иногда контролируемые) хранятся на рабочих станциях и серверах. Таким образом, все хакеры хотят добраться до них, получив доступ к этим критическим активам. Остановка хакера на конечной точке значительно снижает вероятность его успеха, упрощая усилия по разрыву цепочки и значительно повышая эффективность и результативность решений безопасности.



Сервис Panda Adaptive Defense помогает организациям, а также их внутренним и внешним службам обеспечения безопасности повышать свои возможности по предотвращению, обнаружению и реагированию **на угрозы, осуществляя борьбу с ними на всем жизненном цикле кибер-атаки, когда бы они не ударяли по конечной точке**.

Кроме этого управляемый сервис предоставляет данные и знания по каждой угрозе, что позволяет лучше ее оценить и повысить свой уровень безопасности.



2. Понимание Cyber-Kill Chain.

Термин Cyber Kill-Chain изначально был предложен корпорацией Lockheed Martin как часть их модели Intelligence Driven Defense[1] для идентификации и предотвращения процессов кибер-вторжения.

Эта модель определяет, что должны сделать хакеры для того, чтобы достичь своих целей, атакуя сеть, извлекая данные и поддерживая присутствие в организации.

Благодаря этой модели мы знаем, что блокировка хакеров на любом этапе разрывает всю цепочку атаки. Для достижения успеха хакеры должны пройти через все этапы. В свою очередь, нам, обороняющейся стороне, достаточно всего лишь блокировать их на любом этапе, чтобы добиться успеха.

В следующем разделе мы увидим, что конечная точка является неизбежной точкой, через которую идут все атаки, а, следовательно, остановка атаки на этом уровне существенно повышает шансы на противодействие любой кибер-атаке. Вероятность успеха будет выше, если хакеры будут остановлены на ранних этапах.

Кроме того, каждое вторжение, и следы, которое оно оставляет на конечной точке, - это шанс лучше узнать о действиях хакера и использовать это в свою пользу. **Чем лучше мы понимаем хакеров и их способы выполнения атак, тем вероятнее мы сможем построить более эффективную оборону**.

Модель Cyber-Kill Chain указывает на то, что для осуществления своих злодеяний хакеры всегда должны пройти следующие основные этапы:

Внешняя разведка

Этот этап может быть определен как фаза выбора цели, выявления особенностей организации, специфических требований в данной отрасли, выбор технологий, изучения активности компании в соцсетях или через рассылки.

По сути дела, хакер пытается получить ответы на такие вопросы: "Какие методы атаки будут работать с наибольшей степенью успеха?" или, например, "Какие из них будет легче всего осуществить с точки зрения инвестиций и ресурсов?"

Вооружение и упаковка

Возможны различные формы: эксплуатация веб-приложения, стандартные или специально изготовленные вредоносные программы, уязвимости в различных документах (PDF, Office или другие форматы документов) или атаки типа watering hole[2].

Обычно они подготавливаются с очень специфическими знаниями о цели.

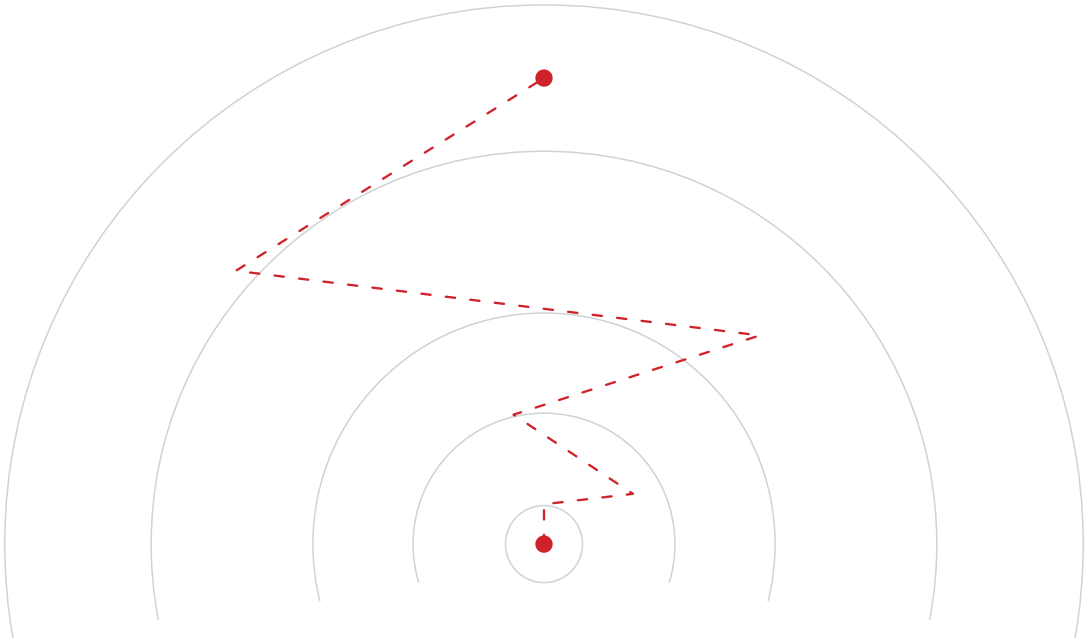
Доставка

Передача требуемого (вредоносного) контента либо по инициативе жертвы (например, пользователь заходит на вредоносный сайт, в результате чего передается вредоносная программ, или он открывает вредоносный PDF-файл), либо по инициативе хакера (SQL-инъекция или компрометация сетевой службы).

Заражение

После доставки на компьютер или устройство пользователя, требуемый (вредоносный) контент разворачивается, устанавливаясь в окружении.

Как правило, это происходит при использовании известной уязвимости, для которой ранее был доступен патч. В большинстве случаев (в зависимости от цели) хакерам не требуется нести дополнительные расходы на поиск и эксплуатацию неизвестных уязвимостей.



Установка

Часто установка происходит на фоне каких-то внешних соединений. Обычно вредоносная программа скрывается в этих операциях, незаметно проникая на конечные точки, к которым можно получить доступ. Затем хакер может контролировать это приложение без ведома жертвы.

Получение управления

На этом этапе хакеры начинают контролировать активы жертвы с помощью таких методов управления (как правило, удаленных), как DNS, Internet Control Message Protocol (ICMP), веб-сайты и социальные сети. В результате, хакер передает на контролируемые "активы" требуемые команды: что делать далее и какую информацию собирать.

Используемые для сбора данных методы: снимки экрана, контроль нажатия клавиш, взлом паролей, мониторинг сети на учетные данные, сбор критического контента и документов. Часто назначается промежуточный хост, куда копируются все данные, а затем они сжимаются/шифруются для дальнейшей отправки.

Выполнение действий у жертвы

На финальном этапе хакер отправляет собранные данные и/или выводит из строя ИТ-активы во время своего нахождения в сети жертвы. Затем проводятся мероприятия по выявлению других целей, расширению своего присутствия внутри организации и (что самое важное) извлечению данных.

Затем цепочка повторяется. Вообще, особенностью Cyber-Kill Chain является то, что она круговая, а не линейная. Как только хакер проник в сеть, он снова начинает эту цепочку внутри сети, осуществляя дополнительную разведку и осуществляя горизонтальное продвижение внутри Вашей сети.

Кроме того, надо иметь в виду, что хотя методология одинакова, но при нахождении внутри сети хакеры будут использовать другие методы для этапов внутренней цепочки, чем в случае, когда они находятся вне сети.

Фактически, после проникновения хакера в сеть, он становится инсайдером (пользователем с определенными правами и присутствием в сети), а это мешает специалистам компании по безопасности подозревать атаку и понимать, что уже идут поздние стадии расширенной модели Cyber-Kill Chain.

Внешняя Cyber-Kill Chain

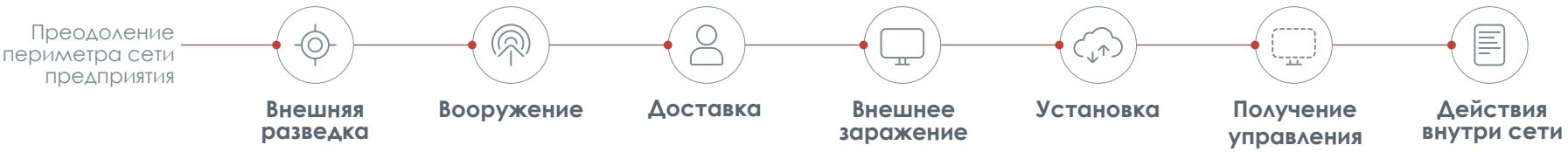


Рис. 1. Диаграмма этапов в Cyber-Kill Chain от периметра до конечной точки. Внешняя Cyber-Kill Chain.

3. Расширенная модель Cyber-Kill Chain.

Cyber-Kill Chain - это круговой и нелинейный процесс, когда хакер выполняет непрерывное горизонтальное продвижение внутри сети. Этапы, которые выполняются внутри сети, такие же, как и те, что выполняются в случае, если цель - получить доступ к сети. Хотя при этом используются различные техники и тактические приемы.

Сочетание внешней и внутренней Cyber-Kill Chain называется расширенной моделью Cyber-Kill Chain. Это означает добавление дополнительных этапов, которые фактически представляют почти такой же набор этапов, только имеют в своем названии слово "внутренний", поэтому Cyber-Kill Chain становится внутренней Cyber-Kill Chain со своими собственными этапами (внутренняя разведка, внутреннее вооружение и т.д.).

Каждый этап атаки после проникновения внутрь сети жертвы может занять от нескольких минут до нескольких месяцев, включая время окончательного ожидания, когда на месте уже все подготовлено и можно начинать атаку.

Отметим, что хакер будет выжидать оптимальное время для запуска атаки, чтобы получить от нее максимальную отдачу.

Этапы разведки и вооружения могут занять несколько месяцев.

Кстати, очень трудно перехватить эти этапы, т.к. они выполняются без соединения с хакером. Именно поэтому очень важно, чтобы средства безопасности на конечных точках анализировали и контролировали все системы и приложения, запущенные на устройствах. Это существенно затруднит работу хакеров, в результате чего атака может стать финансово не выгодна для них.

Внутренняя разведка

На этом этапе хакеры имеют доступ к рабочей станции одного какого-то пользователя, где они будут извлекать данные из локальных файлов, сетевых папок, истории браузера, а также подключаться к Wiki и SharePoint. Цель - выяснить, как эта машина может помочь исследовать сеть и позволить выйти на другие более ценные активы.

Внутреннее заражение

Воспользовавшись недостающими патчами, узявимостями веб-приложений и протоколов передачи данных, спуфингом или даже такими простыми вещами как учетные данные по умолчанию, хакеры смогут перейти от рабочих станций к серверам, используя **расширение прав, горизонтальное продвижение внутри сети, и воздействуя на отдельные целевые машины**.

Рис 2. Расширенная модель Cyber-Kill Chain. Действия для получения доступа к целевой конечной точке и манипуляция ею для достижения поставленной хакером цели.

4. Panda Adaptive Defense в Cyber-Kill Chain.

У хакеров есть цели, и они готовы потратить определенные ресурсы для их достижения. Если механизмы безопасности конечных точек могут повысить стоимость атаки (деньги, люди или время) выше ожидаемой стоимости, тогда хакеры реже будут добиваться успехов или могут даже отказаться от атаки организации.

Именно это и происходит у пользователей, защищенных с помощью Panda Adaptive Defense, ведь миссия Panda Security - это полная защита наших пользователей.

Все организации должны быть готовы к ситуации, когда хакер получил доступ к внутренней корпоративной сети, логинам и паролям, ко всей документации и всем спецификациям сетевых устройств, системам, бэкапам и приложениям, а также быть в состоянии действовать незамедлительно.

Более совершенная стратегия безопасности конечных точек и активов организации необходима для построения более устойчивого предприятия. Она не предотвратит все атаки, но остановит большинство из них на более ранних этапах. Одна из целей - это иметь эффективные механизмы защиты с учетом расширенной Cyber-Kill Chain, чтобы замедлить действия хакеров, сделать процесс развития их атак более дорогим и максимально затруднить их переход на каждый последующий этап.

Если хакеры не могут достичь своих целей экономически оправданным способом, то они переключатся на другие цели или будут достигать аналогичных целей при атаке на другие организации.

Стратегия безопасности организации должна учитывать атаки, осуществляемые не только снаружи, но, что особенно важно, изнутри, т.к. после проникновения хакера внутрь сети, он становится инсайдером с доступом к конечным точкам вместе с их активами.

Традиционный подход к обеспечению безопасности должен быть расширен за счет методов, основанных на понимании Cyber-Kill Chain, и использования технологий, которые способны предотвратить получение хакером доступа к конечным точкам, а также остановить их на любом возможном этапе в рамках внутренней Cyber-Kill Chain.

Наложение стратегии защиты на расширенную модель Cyber-Kill Chain показывает, как организация может предотвращать, выявлять, нейтрализовывать и осуществлять действия по восстановлению на протяжении всех фаз атаки, ориентируя безопасность компании на те же критерии успеха, что используют и хакеры.

Этого трудно добиться в силу целого ряда факторов: приложения становятся все более сложными и взаимосвязанными, они уязвимы, потому что многие программы разработаны без использования строгих принципов безопасности, плюс человеческий фактор. Сотрудники и партнеры также остаются основным вектором риска, а потому здесь есть возможности для атак, основанных на социальной инженерии.

Panda Adaptive Defense и Panda Adaptive Defense 360 учитывают основные факторы, что позволяет компаниям при использовании данных управляемых сервисов **предотвращать и обнаруживать более сложные техники и тактические приемы атак на каждом этапе расширенной модели Cyber-Kill Chain**. Это помогает специалистам по безопасности внутри организации в разработке такой стратегии безопасности, которая будет ориентирована на расширенную модель Cyber-Kill Chain.

5. Основные принципы Adaptive Defense и Adaptive Defense 360.

Предотвращение известных угроз

Поиск известных угроз не защитит от их вариантов или неизвестных атак, но его усиление дополнительными уровнями безопасности способно превентивно останавливать известные угрозы, когда их пытаются внедрить на конечной точке. Panda Adaptive Defense 360 использует обширную коллекцию сервисов репутации для проактивной блокировки хакеров на этапе доставки с использованием данных из облака.

Обнаружение сложного вредоносного ПО

Panda Adaptive Defense и Panda Adaptive Defense 360 обнаруживают и блокируют неизвестное вредоносное ПО и направленные атаки благодаря модели безопасности, основанной на трех принципах: непрерывный глубокий мониторинг всех приложений, запущенных на конечных точках, автоматическая классификация процессов на конечных точках с использованием больших данных и техник машинного обучения на облачной платформе, и возможность глубокого анализа поведения угрозы техническим экспертом в случае, если процесс не классифицирован автоматически.

Динамическое обнаружение эксплойтов[3]

На этапе заражения в расширенной модели Cyber-Kill Chain хакеры используют эксплойты для эксплуатации уязвимостей на уровне кода, благодаря чему они могут взломать приложения и системы, установить и запустить вредоносное ПО. Интернет-загрузки являются распространенным вектором для выполнения атак эксплойтами. Panda Adaptive Defense и Panda Adaptive Defense 360 предоставляют опции динамического анти-эксплойта для защиты от атак на приложения и память.

Panda Adaptive Defense и Adaptive Defense 360 обнаруживают и блокируют актуальные техники, используемые хакерами на этапе заражения (heap spraying, подмена стэка, ROP-атаки и модификации прав памяти...). Также эти решения динамически обнаруживают неизвестные атаки за счет мониторинга всех процессов, запущенных на устройствах, а с помощью корреляции данных через алгоритмы машинного обучения в облаке они способны останавливать любые известные и неизвестные попытки заражения.

Анти-эксплойтные технологии в Adaptive Defense останавливают хакеров на ранних стадиях внутренней атаки, обнаруживая момент компрометации надежного приложения/процесса.

Смягчение атаки

Защита конечных точек следующего поколения должна предотвращать и обнаруживать хакеров на различных этапах Cyber-Kill Chain, однако обнаружение должно сопровождаться быстрым смягчением атаки на ее начальных этапах.

Panda Adaptive Defense 360 автоматически и своевременно смягчает атаку, помещая на карантин вредоносные программы, останавливая скомпрометированные процессы или даже полностью выключая систему для минимизации ущерба.

Восстановление

Во время своего выполнения вредоносные программы часто создают, модифицируют или удаляют системные файлы и настройки реестра, а также меняют параметры конфигурации.

Эти изменения или остатки, которые могут остаться после, могут вызвать неисправности системы или даже "открыть дверь" для новых атак.

Panda Adaptive Defense 360 восстанавливает конечные точки в свое устойчивое положение до заражения вредоносными программами.

Экспертная информация

Во время сильно меняющегося "пейзажа" угроз, их частоты появления, сложности и направленной природы хакеров, не может быть ни одной технологии безопасности, гарантирующей 100% эффективность, а потому должна быть возможность получения экспертной информации по каждой конечной точке в реальном времени для обеспечения полной видимости.

Сотрудники отделов информационной безопасности на предприятиях должны иметь внедренный план по борьбе с нарушениями работы систем отчетности, по взаимодействию с правоохранительными органами и пр.

Panda Adaptive Defense и Panda Adaptive Defense 360 предоставляют четкий и своевременный обзор вредоносной активности внутри организации. Такая видимость позволяет специалистам компаний по безопасности быстро оценивать масштабы атаки и предпринимать соответствующие действия.

Рис. 3. График жизненного цикла атаки в рамках экспертного анализа.

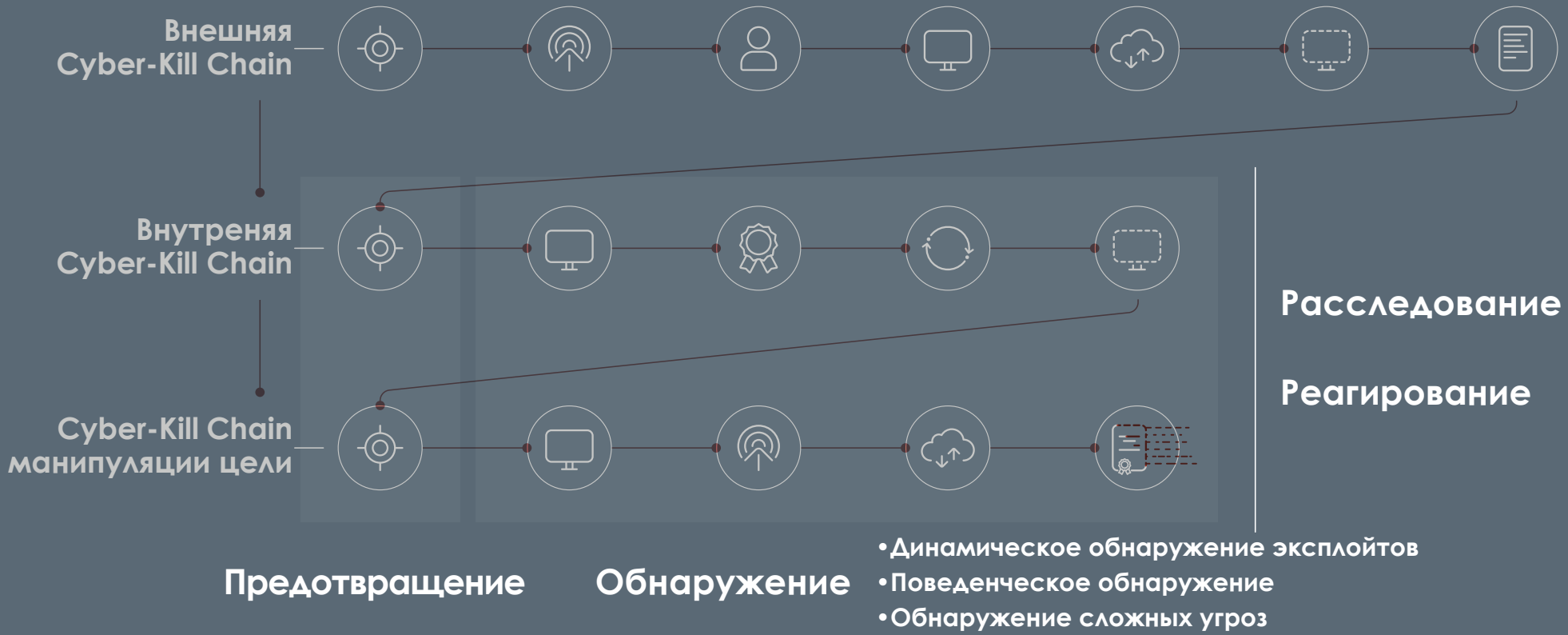


Рис. 4. Основы безопасности Adaptive Defense 360 для расширенной модели Cyber-Kill Chain.

Ссылки.

- Lockheed Martin's Cyber-Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, at Black Hat 2016: Extended Cyber kill chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 07 April 2016

[1.] Eric M. Hutchins,Michael J. Cloppert, and Rohan M.Amín, Ph.D.,Intellígence-Dríven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kili Chains.

[2.] **Атаки типа watering hole (водопой)**. Специфический тип направленной атаки, когда жертва принадлежит к определенной группе (организация, сфера деятельности или регион). В этой атаке хакер определяет набор веб-сайтов, которые часто посещают члены этой группы, и заражает один или несколько из них вредоносными программами. В конечном итоге, заражаются некоторые члены этой группы.

Вредоносные программы, используемые в таких атаках, обычно собирают информацию о пользователе. Хакеры, осуществляющие поиск специфической информации, могут атаковать пользователей только с определенного IP-адреса. Хакера сложнее обнаружить и изучить. Название данного типа атаки связано с хищниками в природе, которые ожидают возможности атаковать свою жертву рядом с водопоем.

Опора на веб-сайты, которым доверяют члены группы, делает такую стратегию весьма эффективной, даже при атаке тех групп, которые устойчивы к целевому фишингу (spear phishing) или другим формам фишинга.

[3.] **Динамическое обнаружение эксплойтов**. Это инновационная технология компании Panda Security, основанная на мониторинге всех запущенных процессов на конечной точке или сервере и их анализе в облаке с помощью технологий машинного обучения (ML), ориентированных на обнаружение попыток применения эксплойтов к надежным приложениям.

Эта новая технология предназначена для остановки атак на рабочие станции и серверы на самых ранних этапах Cyber-Kill Chain. Сдерживание хакеров и затруднение их доступа к устройству до такой степени, что теряется экономический смысл атаки, будут препятствовать дальнейшим попыткам осуществления атаки. В конечном итоге, это значительно повысит уровень обнаружения.

Подробнее:

pandasecurity.com/intelligence-platform/

+7 495 105 94 51

sales@rus.pandasecurity.com

panda