cezurity

Выявление и интерпретация аномалий при детектировании сложного вредоносного ПО и целенаправленных атак (APT)

Справочный документ

Данный документ описывает некоторые способы выявления и интерпретации аномалий как одного из ключевых признаков для обнаружения сложного вредоносного программного обеспечения и целенаправленных атак (APT). Документ носит ознакомительный характер и предназначен для иллюстрации работы технологии, а не детального ее описания.

Аномалии. Уровни аномалий

Под **аномалиями** обычно понимается отклонение от нормы, от общей закономерности, “неправильность”.

Существует несколько уровней аномалий:

1. Аномалии в контексте среза одной отдельно взятой исследуемой системы.
2. Аномалии в контексте ретроспективы срезов одной отдельно взятой исследуемой системы.
3. Аномалии в контексте ретроспективы срезов набора исследуемых систем.

Выявленная аномалия не обязательно приводит систему в alertable состояние , все зависит от ее “веса” – некоторой сторонней оценки важности аномалии. Эти задачи решает экспертная система или аналитик.

На каждом последующем уровне может использоваться информация, полученная на предыдущем, – она может усилить “вес” аномалии текущего уровня и привести к срабатыванию системы.

Аномалии, о которых здесь пойдет речь, относятся к видам анализа, описанным в документе “Технология динамического обнаружения целенаправленных атак”.

Аномалии в контексте среза одной отдельно взятой исследуемой системы

В рамках этого исследования мы анализируем отдельно взятый срез системы на предмет:

Аномалий в рассматриваемых независимо друг от друга объектах системы, к примеру:

- Нетипичные для легитимного ПО наборы характеристик объектов системы. С помощью облачной технологи Cezurity Cloud непрерывно пополняется обширная база знаний об объектах и их характеристиках, встречаемых на ПК

пользователей, информацию об их априорной принадлежности к какому-либо классу ПО. Основанная на этих данных классифицирующая система выделяет нетипичные для легитимного ПО наборы характеристик и использует их для создания классификатора средствами машинного обучения (Machine Learning, ML), в дальнейшем используемого для выявления объектов с такого рода аномалиями.

Пример: объект исследуемой системы, обладающий следующими характеристиками – упакованный исполняемый файл без цифровой подписи и информации об авторстве, прописанный в автозагрузку, имеющий низкую или близкую к нулевой распространенность. Такого рода объект будет однозначно классифицирован системой как имеющий аномалии.

- Противоречивые наборы характеристик объектов системы. Используя информацию, накопленную в Cezurity Cloud, решение располагает сведениями о наборах характеристик разнообразного легитимного ПО. Для выявления противоречий производится классификация исследуемого объекта, посредством искусственно ограниченного подмножества характеристик, после чего выявляются аномалии, с учетом полного набора характеристик исследуемого объекта и характеристик объектов класса, полученного на предыдущем шаге.

Пример: вредоносный файл, подписанный легитимной цифровой подписью и имеющий популярное имя и размер, при этом его статические характеристики или местоположение в системе отличаются от характерных для подобного класса объектов. Налицо аномалия.

- Несовпадение в одних и тех же наборах характеристик объекта, полученных разными способами. Этот механизм эффективно выявляет наличие rootkit-компонент целенаправленных атак (Advanced Persistent Threats) и разнообразных сложных угроз, стремящихся быть незамеченными на целевых ПК.

Аномалий в рассматриваемых совместно объектах системы, к примеру:

- Противоречия в наборе объектов системы. Объекты системы часто логически связаны между собой, и наличие одних бессмысленно без присутствия других. Как и наоборот, присутствие некоторого объекта делает невозможным (с точки зрения работоспособности системы) или бессмысленным присутствие другого. Облако Cezurity Cloud непрерывно пополняется информацией о возможных совместных и несовместных сочетаниях объектов, и их характеристиках в рамках одной системы, что позволяет выявить подложный объект, выдающий себя за компонент какой-либо более сложной системы.

Пример: если известно, что ПК оборудован сетевой картой Realtek, то, в этом случае, в срезе будет наблюдаться целый набор файлов, относящихся к вендору Realtek. Но появление только лишь одного файла драйвера, при отсутствии прочих, делает такой файл крайне подозрительным.

Аномалии в контексте ретроспективы срезов одной отдельно взятой исследуемой системы

В рамках этого исследования анализируется совместно набор срезов отдельно взятой системы на предмет:

Аномалий в локализованных изменениях наборов объектов системы, представленных срезами (slice). На этой фазе неважно итоговое состояние объекта – каждое изменение его характеристик рассматривается независимо:

- Изменение характеристик существующих объектов. Причиной изменений характеристик объектов могут быть такие нелегитимные изменения, как например:

  – заражение объекта файловым вирусом;
  – внедрение в исходно легитимный объект вредоносного кода с целью затруднения обнаружения атаки;
  – порча объекта в результате неправомерного изменения, к примеру, для обезвреживания существующих средств защиты ПК;
  – изменение внешних характеристик существующих объектов (локаций, веток реестра, ключей командной строки) с целью придания им новой функциональности.

  Любые изменения существующих объектов отслеживаются системой и анализируются с целью установления характера изменения. Это важно, так как изменения в характеристиках объектов могут быть и правомерными – обновления программ, изменение конфигурации ПК, появление новых легитимных объектов, штатно модифицирующих некоторые характеристики существующих. Анализ такого рода изменений заключается в:

  – преобразовании изменения в некоторый формальный вид, обладающий в достаточной степени инвариантностью, и, тем самым, позволяющий агрегировать схожие типы изменений в один вектор запроса;
  – далее, система ищет схожие вектора в постоянно пополняемой облачной базе данных Cezurity Cloud и ранжирует их в порядке убывания схожести;
  – по результатам k “типов изменений” (аномальные – неаномальные), описываемых наиболее похожими векторами, берутся в качестве “рабочего набора” гипотез характера исследуемого изменения;

– в случае непротиворечивости негативных гипотез, изменение может быть признано серьезной аномалией уже на этом этапе исследования. В противном случае, результат исследования будет использоваться в дальнейшем анализе.

Пример: изменение существующего в системе файла с целью получения механизма автозапуска вредоносного кода, которое достаточно просто отличить от штатного обновления, обладая знанием об исходных характеристиках объектов.

Аномалий в локализованных изменениях наборов объектов системы, представленных слайсами. На этой фазе рассматриваются изменения глобально, в контексте всей системы:

- Исчезновение и появление новых объектов. Появление новых неизвестных объектов в системе является одним из характерных признаков целенаправленной атаки (APT). При грамотном ее проведении, появление объектов растянуто во времени – по этой причине классические системы теряют новые объекты из контекста обнаружения и оценивают их независимо друг от друга. Таким образом, условие, при котором произойдет перевод системы в alertable состояние, тождественно переводу в alertable состояние самым небезопасным, с точки зрения системы защиты, объектом. Исчезновение объектов также является важным с точки зрения определения вторжения – к примеру, это может быть удаленные файлы баз антивирусов, критическое системное ПО и т.п. Рассматриваются все новые и исчезнувшие объекты в совокупности, с учетом результатов анализа, проведенного в предыдущих пунктах, и базы знаний в облаке Cezurity Cloud. Всем типам событий выдаются веса, оценивается общий уровень опасности. По результатам система может быть переведена в alertable состояние или анализ может быть продолжен на следующем шаге.

  Пример: появление в системе нескольких условно-легальных "хакерских" утилит для обеспечения удаленного доступа, сбора паролей и т.п., а также некоторого набора скриптов для автоматизации их работы. В классическом подходе каждый объект сам по себе не вызвал бы подозрений, и система не была бы переведена в alertable состояние.

- Изменение характеристик существующих объектов. Пункт схож с пунктом, в котором рассматривается каждое изменение характеристик независимо, за исключением следующих ситуаций:

  – характеристики объектов менялись неоднократно и, в результате изменение было нивелировано. Исходный объект совпадает с последней версией, представленной срезом (slice). Такое поведение анализируется облаком, и может как снизить, так и наоборот повысить вклад веса изменений объекта в факт определения аномалии в зависимости от класса, присвоенного аналитическим компонентом облака: обновление ПО с

последующим откатом, лечение файлового вируса, сокрытие следов атаки, уничтожение “улик” и т.п.

– характеристики объектов менялись неоднократно и ни одна из пар независимых изменений не совпадает с изменением исходного объекта к его текущему состоянию. В этом случае мы формируем глобальное изменение объекта и далее поступаем с ним так же, как и в локальном случае.

Пример: попытка сокрытия следов проведенной атаки путем коррекции измененных веток реестра, атрибутов файлов или перемещение объектов в исходные локации.

Аномалии в контексте ретроспективы срезов набора исследуемых систем

В рамках этого исследования анализируются совместно наборы срезов исследуемых систем на предмет аномалии в изменениях наборов слайсов исследуемых систем.

Для целенаправленных атак (APT) характерна локализованность в рамках нескольких ключевых инфраструктурных элементов. К примеру, это может быть ПК в бухгалтерии, в случае попытки проведения финансовых махинаций, или ПК главного разработчика, начальника отдела – в случае попытки кражи интеллектуальной собственности. Остальные объекты организации, как правило, остаются не затронуты, либо их количество невелико – они используются как “трамплины” для достижения поставленной цели. Опираясь на этот факт, оценивается корреляция между аномалиями (изменениями), выявленными на предыдущих этапах исследования систем в рамках всего парка машин предприятия. Тем самым, аномалии, выявленные на предыдущем этапе, могут как усилить свой вес, в случае отсутствия значимых корреляций, так и наоборот уменьшить, если таковые найдены.

Россия, Санкт-Петербург
ул. Матроса Железняка, 57

+7 812 640 4143
www.cezurity.com