ANGARA
Professional Assistance

Отчет Центра киберустойчивости Angara Cyber Resilience Center (ACRC) за I полугодие 2019 года

КОНТАКТЫ

121096, г. Москва, ул. Василисы Кожиной, д.1, к.1.
БЦ «Парк Победы»
Телефон: +7 (495) 269 26 06
E-mail: info@angarapro.ru

Введение

Отчет основан на статистике, собираемой компанией Angara Professional Assistance в рамках предоставления услуг по мониторингу и управлению инцидентами информационной безопасности (ИБ) на базе Центра киберустойчивости Angara Cyber Resilience Center (далее – «Центр киберустойчивости»).

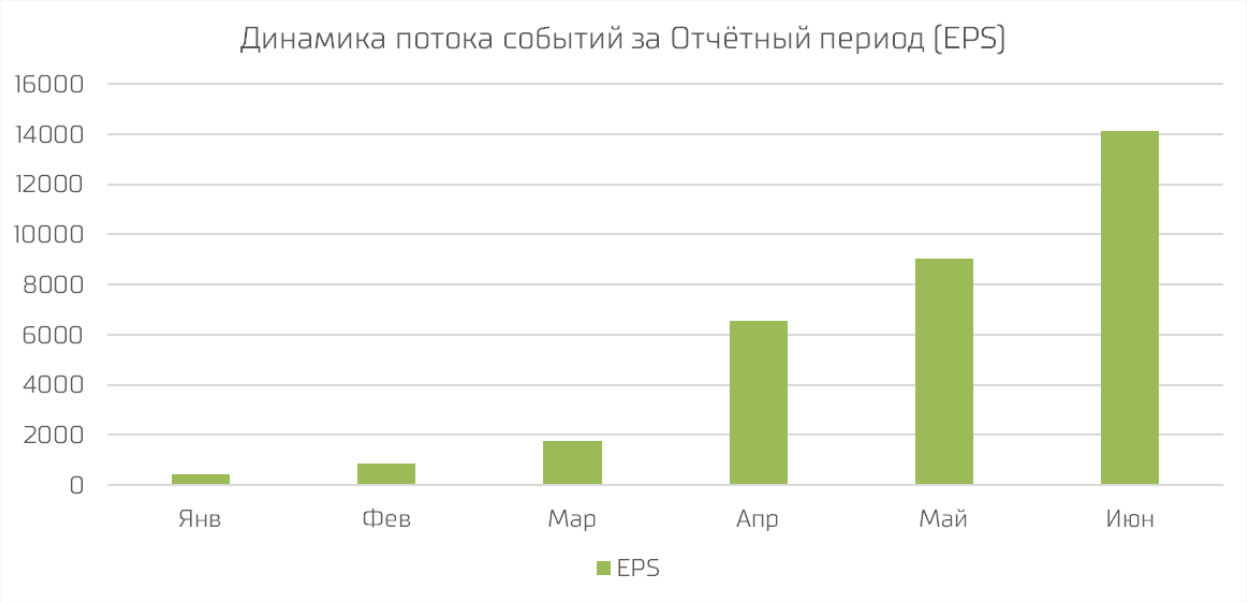
Термины и определения, используемые в отчете при подсчете статистики:

1.	EPS (Events per Second)	Количество событий в секунду.
2.	Событие	Любое событие, связанное с изменением состояния Системы (изменение конфигурации, появление новых пользователей или компьютеров, запуск программных процессов, установка сетевых соединений и т.п.).
3.	Источник события	Программные средства или программно-аппаратные средства, генерирующие события.
4.	Подозрение на инцидент	Непредвиденное или нежелательное событие, которое может быть признаком Инцидента.
5.	Инцидент	Непредвиденное или нежелательное событие, негативное влияние которого на деятельность информационных систем достоверно установлено.

В рамках услуг Центром киберустойчивости обеспечивается автоматизированная обработка принимаемых Событий ИБ с целью их агрегирования и ранжирования, с последующей экспертной оценкой аналитиками ACRC. Аналитики присваивают каждому правилу параметры, такие как достоверность, опасность и приоритет. Для каждого клиента параметры являются индивидуальными. Из общего объема Событий ИБ производится выборка событий, потенциально оказывающих влияние на уровень информационной безопасности клиента. Похожие события группируются по типам.

Статистика по полученным данным

За период с января по июнь 2019 г. поток принимаемых и обрабатываемых событий (EPS) в Центре киберустойчивости значительно вырос до 14127 EPS в июне:



За первое полугодие 2019 года мы обогатили нашу платформу более 20 новыми коннекторами к разным системам, которые используют наши клиенты. Среди них коннекторы к системам таких производителей, как Varonis Systems, Proofpoint, Код безопасности, Illusive Networks и др.

Также нам удалось проверить работу ACRC в экстремальных условиях – мы обеспечили возможность передачи данных без потерь через спутниковые каналы связи, работающие с большими задержками.

Статистика по подозрениям на инциденты

В процессах мониторинга мы используем собственную модель «Cyber-Kill Chain», которая является упрощенной моделью MITRE, адаптированной на основе нашего опыта для организаций на территории РФ. Процессы мониторинга выстроены таким образом, чтобы максимально повысить вероятность выявления атак на ранних стадиях. На основе собственной матрицы признаков атак мы фиксируем каждое срабатывание правил автоматического выявления и формируем Подозрение на инцидент, приступая к расследованию для его подтверждения или опровержения.

В «топ» наиболее популярных инцидентов попали: заражение вредоносным ПО, доставка вредоносного ПО через email и брутфорс. В современном мире, когда такие средства, как WAF и NGFW не являются редкостью, злоумышленники пытаются всеми возможными способами проникнуть в корпоративную сеть через самое уязвимое звено – пользователя. К сожалению, определенный процент этих атак достигает своей цели, но, практически, не находит дальнейшего развития, так как легко детектируется.

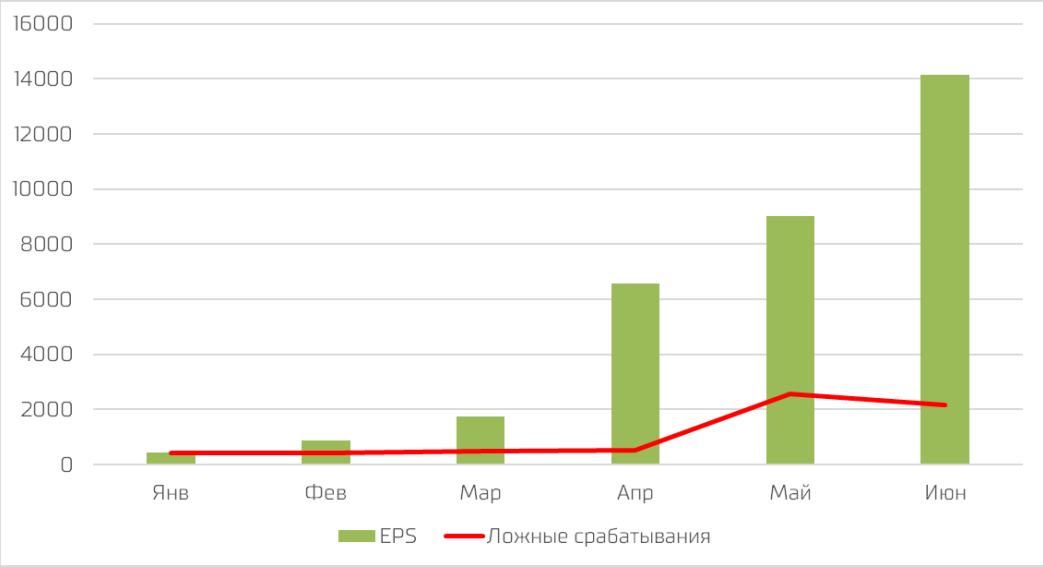
Статистика подтвержденных инцидентов

Далеко не каждое подозрение на инцидент подтверждается. Оказывая услуги, мы стараемся соблюдать баланс вовлеченности персонала клиентов в расследование подозрений на инцидент: расследование ведется в соответствии с SLA, при этом мы не переносим ответственность за решение о ложноположительном срабатывании на клиента. Одной из ценностей коммерческих SOC, по отношению к in-house решениям, является возможность анализа статистики и трендов на множестве данных клиентов. Мы делимся выводами по результатам такого анализа для повышения общего уровня безопасности в РФ и мире.

Среди подтвержденных инцидентов на первом месте мы наблюдаем инциденты с заражением вредоносным ПО, что лишний раз акцентирует внимание на том, что данную угрозу нельзя игнорировать. Также в «топ» подтвержденных инцидентов входят нелегитимная аутентификация и ошибки конфигурации информационных систем. В больших инфраструктурах, где обеспечение непрерывности бизнес-процессов является приоритетной задачей, служба эксплуатации, к сожалению, зачастую, не может полностью придерживаться всех регламентов и стандартов информационной безопасности. Одна из ценностей центра мониторинга состоит как раз в оповещении службы безопасности об инцидентах ИБ. Часто именно эта информация говорит нашим клиентам о том, где надо подкрутить «гайки» в системе безопасности.

Статистика по работе аналитиков центра

С ростом количества событий ИБ количество подтвержденных инцидентов не становится больше, скорее наоборот, чем лучше мы узнаем клиента, тем точнее нам удается понять, что происходит в его инфраструктуре. Клиент же получает возможность скорректировать свой Security Baseline, учитывая выявленные в ходе мониторинга отклонения. Решение об отнесении к ложному срабатыванию может быть принято автоматически на основе логики фильтрации, согласовываемой с клиентом, при этом совершенствование работы фильтров производится непрерывно, в постоянном взаимодействии с клиентом.



Тенденции

На протяжении нескольких лет трендом среди кибератак являются таргетированные атаки, но это не повод уделять менее пристальное внимание классическим видам атак. Согласно статистике нашего Центра киберустойчивости, наибольшее количество атак проводится с куда более прозаичной целью – такой как, например, майнинг. Тем не менее, наши аналитики отмечают, что фрод становится более массовым и изощренным. Пользователи хотят открыть письма, даже если проводилась обыкновенная массовая рассылка. Как ни странно, запароленные архивы вызывают куда больший интерес работников, чем обычные вложения.

Интересный кейс

В рамках предоставления нашей услуги, мы обязательно используем систему предотвращения вторжений. Это позволяет аналитикам выявлять аномалии трафика. Отдельно нужно отметить что установка агента ACRC на рабочей станции не является обязательной для того, чтобы аномалией заинтересовался аналитик.

В одну из рабочих смен нашей бдительной команды как раз и произошло такое событие. Анализ netflow выявил подозрительную активность: один из хостов клиента, не содержащий агента ACRC, осуществлял попытки связи с командным центром ботнет-сети. Аналитик выяснил, что, согласно индивидуальным правилам сетевого разграничения, характерным для конкретного клиента (security baseline), хост должен находиться в специализированном, «закрытом» сегменте сети и, соответственно, никак не должен себя проявлять на «радарах мониторинга». По результатам анализа было выяснено, что хост не просто находится в неправильном сегменте, так еще к нему можно подключиться по http напрямую из Интернета, минуя все средства защиты информации. Об инциденте был проинформирован клиент.

По результатам расследования было выяснено, что сотрудники клиента, тестировавшие новое программное обеспечение, ушли домой, забыв выключить IIS и включить антивирусное средство. Команда реагирования со стороны клиента устранила проблему практически мгновенно – хост вернулся в «защищенную гавань», антивирус запустили, IIS выключили. Этот случай еще раз иллюстрирует всем известную поговорку – «доверяй, но проверяй». Даже если вы уверены, что ваша инфраструктура уже отлично защищена и есть сегменты, лишенные сетевого взаимодействия с сетью Интернет, это не повод не производить мониторинг наличия запрещенного взаимодействия.

О группе компаний Ангара

Angara Professional Assistance — это высокотехнологичный сервис-провайдер широкого набора тиражируемых услуг кибербезопасности (MSSP).

В фокусе компании: сервисы по модели Security as a service, аутсорсинг информационной безопасности, услуги по сопровождению и поддержке работоспособности ИТ- и ИБ-систем клиентов, повышению эффективности их работы и обеспечению непрерывности выполняемых функций.

Команда Angara Professional Assistance насчитывает более 50 экспертов в области поддержки и мониторинга информационных инфраструктур с опытом оказания услуг для крупнейших компаний нефтегазового, финансового и государственного секторов.

Квалификация экспертов подтверждена сертификатами авторитетных международных организаций (CEH, CISA, ITIL Expert).

Angara Technologies Group специализируется на проектировании, внедрении и сопровождении систем и решений в области информационной безопасности, помогая совершенствовать процессы и повышать устойчивость информационных и технологических инфраструктур.

Свою миссию компания видит в том, чтобы помочь как можно большему числу своих клиентов не отвлекаться на угрозы и вызовы цифрового мира, позволив им сосредоточиться на своих основных, первостепенных задачах.

Документ подготовлен Центром киберустойчивости «Ангара ассистанс»
С описанием услуг Вы можете ознакомиться на сайте: https://www.angarapro.ru/

2019 г.