ANGARA
professional assistance

Отчет Центра киберустойчивости Angara Cyber Resilience Center (ACRC) за I полугодие 2020 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

Содержание

Введение 3

1 Статистика по данным 4

2 Статистика по подозрениям на инциденты 5

3 Статистика подтвержденных инцидентов 6

4 Статистика по работе аналитиков центра 9

5 Управление правилами автоматизированного выявления 10

Заключение 12

О группе компаний Angara 13

Истории успеха 13

Введение

Настоящий документ представляет собой отчет, основанный на статистике, собираемой ООО «Ангара ассистанс» в рамках предоставления услуг по мониторингу и управлению инцидентами информационной безопасности (ИБ) на базе Центра киберустойчивости Angara Cyber Resilience Center (далее – «Центр ACRC», «Центр киберустойчивости»).

Термины и определения:

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

В рамках процесса предоставления услуг Центром киберустойчивости обеспечивается автоматизированная обработка принимаемых Событий ИБ с целью их агрегирования и ранжирования для последующей экспертной оценкой аналитиками ACRC.

Мониторинг Событий ИБ осуществляется по двум основным сценариям: Alerting и Hunting.

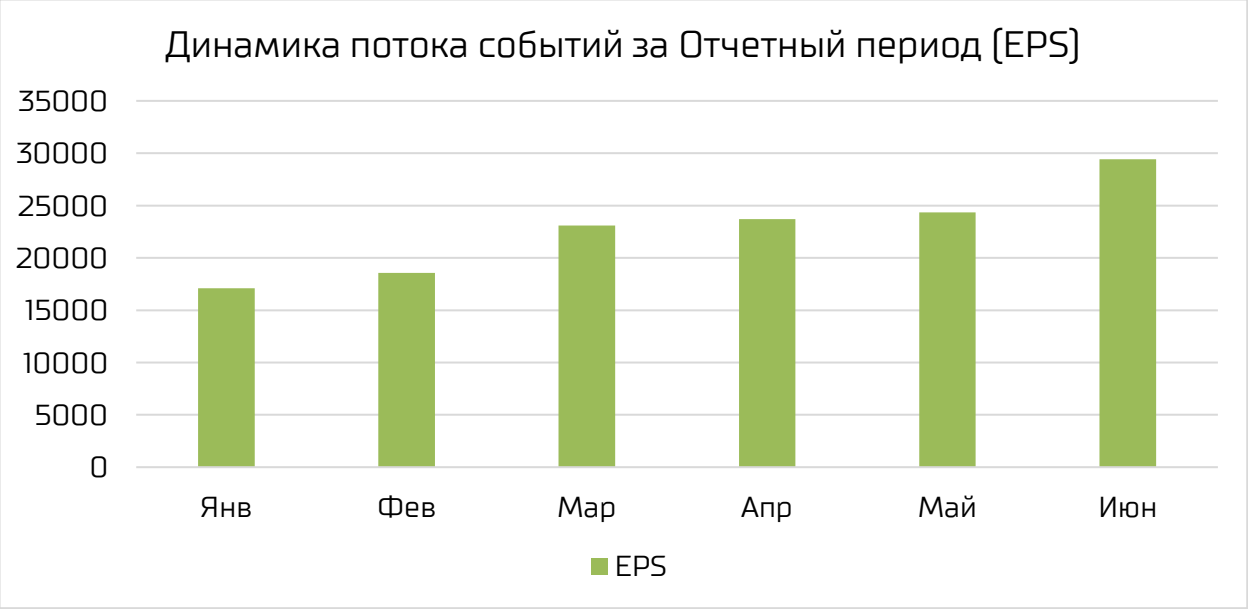
Alerting – метод, при котором поиск признаков различных атак осуществляется по разработанным правилам. Основную работу выполняет платформа ACRC, позволяющая автоматизировано обрабатывать большой поток данных и выявлять Подозрения на инциденты. Данные события требуют «ручного» анализа аналитиками ACRC с целью подтверждения или опровержения конкретного Подозрения на инцидент.

Hunting – метод анализа событий путем выявления нетипичной активности в работе определенных информационных систем (ИС), сетевом трафике и прочих событиях, обрабатываемых при мониторинге. Данный метод реализуется преимущественно «вручную» наиболее опытными аналитиками ACRC. Используются различные средства визуализации событий (диаграммы, графики) и системы эвристического анализа с применением техник искусственного интеллекта. При выявлении различных аномалий собирается дополнительная информация для подтверждения Инцидента ИБ. Новые способы выявления различных угроз впоследствии автоматизируются и в результате добавляются в пакет экспертизы ACRC в виде новых правил или других внутренних ресурсов платформы ACRC.

1 Статистика по данным

За I полугодие 2020 года средний поток событий, обрабатываемых Центром ACRC после фильтрации, составил 23 000 EPS. При подсчете этих статистических данных не учитывался поток событий NetFlow, так как в подавляющем большинстве случаев данные события используются для обогащения информации при расследовании Инцидентов ИБ.

Несмотря на подключение новых клиентов, аналитикам удалось сохранить поток на уровне прошлого полугодия благодаря регулярным мероприятиям по анализу и оптимизации потока входящих данных. Это позволяет оперировать только полезным потоком событий, но, вместе с тем, события, которые прямо сейчас не требуются для выявления признаков атак и инцидентов, могут в будущем составлять основу новых правил, свидетельствующих о применении новых тактик и техник злоумышленника. Если аналитики ACRC видят необходимость использования дополнительных данных или событий для выявления угроз при расследовании Подозрений на инциденты, то фильтрация данных у клиента перенастраивается.



2 Статистика по подозрениям на инциденты

Пандемия наложила отпечаток на статистику Подозрений на инциденты. Большая часть Подозрений касалась установки средств удаленного администрирования, использования хакерских утилит и эксплуатации уязвимостей. Также аналитиками фиксировались множественные факты доставки вредоносного ПО (ВПО) через e-mail (отражено в таблице Подозрения на инцидент ИБ – Доставка: Доставка ВПО через e-mail). Большое количество фишинговых атак было связано с наиболее горячими темами: COVID-19 и всероссийское голосование по поправкам в Конституцию, которые позволяют злоумышленникам заинтересовать большое количество пользователей и вынудить их перейти по ссылкам или открыть прикрепленные вложения. Благодаря оперативной реакции на События ИБ, как со стороны аналитиков, так и со стороны клиентов, реализации угроз за отчетный период удалось избежать.

Почти по всем типам Инцидентов прослеживается изменение профиля поведения. Часть из них хорошо иллюстрирует упомянутые выше тенденции, по некоторым наблюдается спад: несмотря на рост количества опубликованных в сети Интернет сервисов и информационных систем вследствие перехода на удаленный режим работы, количество регистрируемых попыток неуправляемой (автоматической) вредоносной активности снизилось. Частота случаев сетевого сканирования и неуспешных атак подбора пароля методом перебора не изменилась, однако для смещения фокуса внимания скоринг этих кейсов был снижен, так как нередко такая вредоносная активность является отвлекающим маневром. Подробное описание причин указанных изменений по каждому кейсу приводится далее для подтвержденных инцидентов.

3 Статистика подтвержденных инцидентов

Приведенный отчетный период охватывает время, когда компании в экстренном порядке переходили на режим удаленной работы, и процесс не везде можно назвать «гладким».

Большое количество ВПО было скачано пользователями под видом легитимных приложений (в том числе игровое ПО, средства для взлома ПО, мессенджеры и т.д.). Подобные инциденты, непосредственно связанные с удаленной работой, составили 12% от всех событий, относящихся к ВПО. Увеличение их количества вызвано прямым доступом в сеть Интернет в обход корпоративных средств анализа веб-трафика.

Также в период удаленной работы фиксировалось большое количество установок на корпоративные рабочие станции таких нелегитимных средств удаленного администрирования, как Radmin, TeamViewer и Ammyy Admin. Наделенные полномочиями администратора пользователи производили непосредственно инсталляцию ПО, пользователи, лишенные этой возможности, пользовались ПО, не требующим установки (portable) и предварительно скачанным из недоверенных источников.

Часть наших Клиентов решила пойти по пути стратегии BYOD, когда сотрудники используют личные устройства (личный ПК или ноутбук) для подключения к корпоративной сети средствами удаленного доступа. Обычно для подключения подобных ПК на них устанавливается такой минимальный набор средств защиты информации (СЗИ), как система антивирусной защиты и HIDS, которые позволяют выявить вредоносную активность на хостах пользователей. Но, в некоторых случаях, пользователи подключались к корпоративной сети без необходимых СЗИ, что является нарушением политик информационной безопасности. Зараженные хосты без

необходимых СЗИ выявлялись по подозрительной сетевой активности, регистрируемой системами IDS, и обращениям к ресурсам с плохой репутацией, согласно индикаторам компрометации (IOC).

Во время удаленной работы регистрировалось несколько инцидентов, связанных с эксплуатацией таких уязвимостей, как CVE-2019-0708 (BlueKeep) и CVE-2017-0144 (EternalBlue) протоколов RDP и SMB на корпоративных хостах. В ходе расследования выяснилось, что хостам выдавались «белые» адреса сети Интернет для работы из дома, что позволило внешним злоумышленникам осуществить попытки эксплуатации уязвимостей.

В результате экстренного перехода на удаленную работу выросло количество ошибок конфигурации на сетевом оборудовании. У части клиентов был открыт доступ из сети Интернет к сервисам, которые не предназначены для публичного доступа. Злоумышленники, воспользовавшись ситуацией, пытались осуществить попытки подбора пароля к сервисам и эксплуатации уязвимостей.

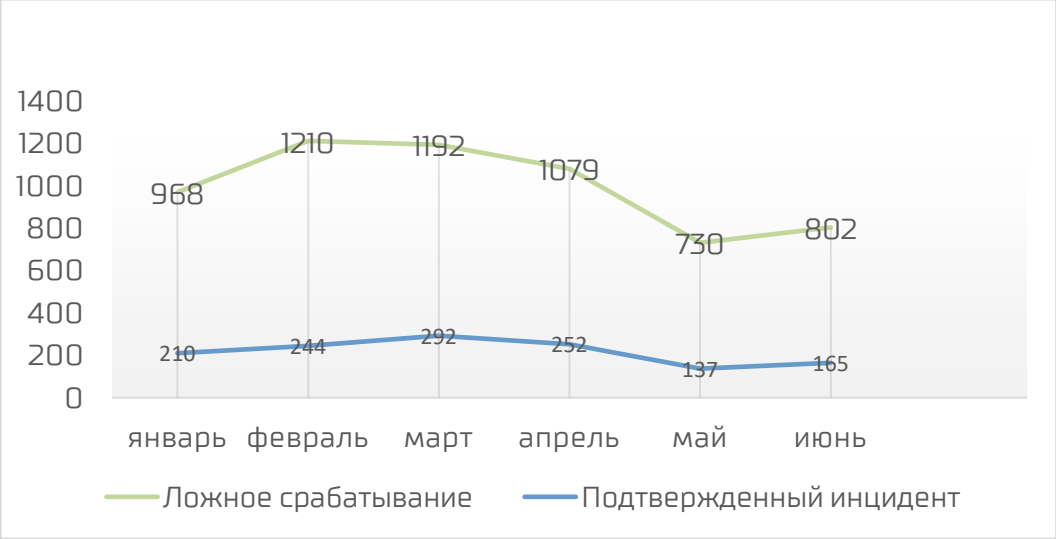
Нельзя не отметить такой дешевый способ доставки вредоносного ПО, как фишинг. Аналитики ACRC фиксируют большое количество фишинговых писем на корпоративные адреса компаний, содержащих вредоносные вложения или ссылки на вредоносный контент. Чаще всего вредоносное вложение доставляется в архиве с паролем, что позволяет обойти проверку содержимого средствами антивирусной защиты на почтовом сервере. Одна из заметных фишинговых рассылок была замаскирована под запрос Федеральной налоговой службы России: пользователь получал письмо от адресата info@nalog.ru с темой «Запрос ФНС». Во вложении находился исполняемый файл, который при запуске инициировал установку средства удаленного администрирования Remote Manipulator System (RMS), которое злоумышленники давно используют для управления скомпрометированными хостами. Данное ПО является легитимным, так как производится доверенным производителем, и может использоваться по назначению ИТ-администраторами. Средства антивирусной защиты не фиксируют Подозрений для данного типа ПО, если это не настроено принудительно. Выявить такую активность можно, если запуск подозрительных файлов из почтовых вложений подлежит проверке аналитиками.

Все вышеперечисленные тренды можно наглядно увидеть в сравнении периодов II полугодия 2019 года и I полугодия 2020 года:

Стоит отметить возросшую статистику по инцидентам типа «Заражение ВПО». Это связано с тем, что ранее аналитиками ACRC не регистрировались инциденты, связанные с успешным обнаружением и устранением угрозы антивирусными средствами, если это не являлось частью более сложного вектора атаки или не свидетельствовало о нарушении принятых политик безопасности. С середины марта было решено регистрировать инциденты подобного типа с целью комплексного анализа ситуации на удаленных рабочих станциях, ведь рано или поздно они должны были вернуться в защищенный периметр.

4 Статистика по работе аналитиков центра

Доля подтвержденных Инцидентов осталась на уровне прошлого полугодия и составила 13%. В мае зафиксировано не только существенное сокращение количества Подозрений на инциденты, но и снижение количества подтвержденных Инцидентов. Это связано с длительными майскими праздниками, началом периода отпусков у большинства наших Клиентов и стабилизацией перехода на удаленную работу.



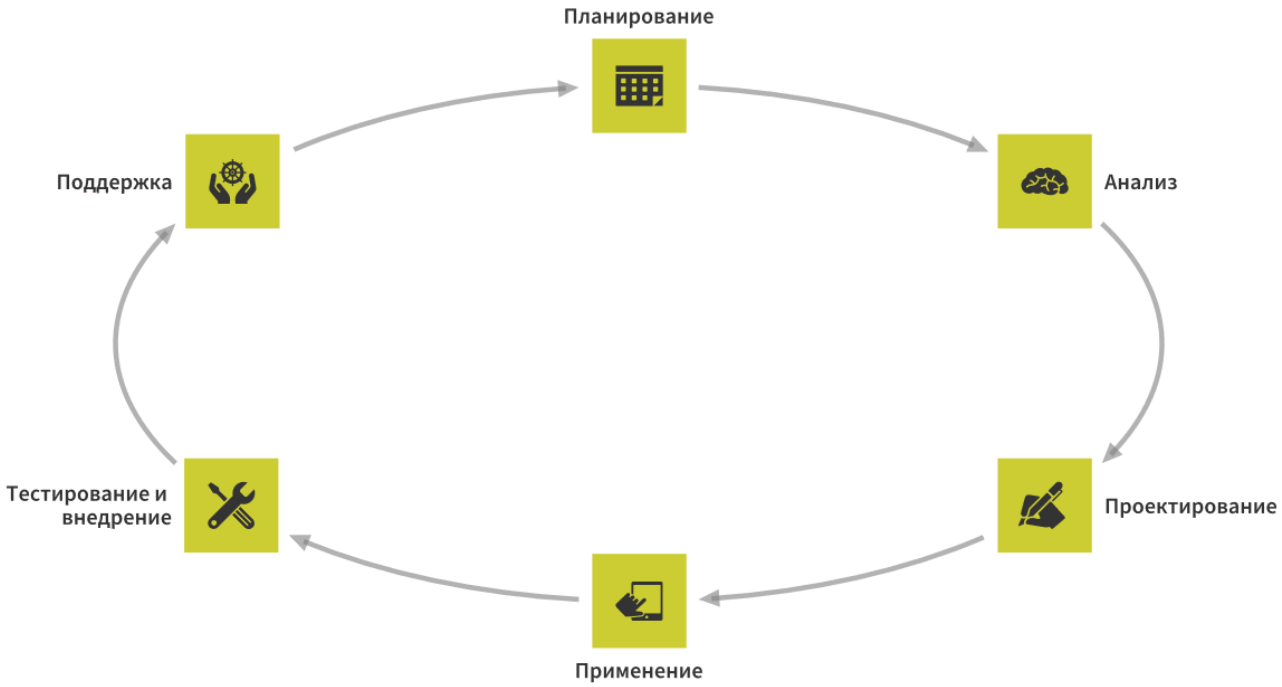
В процессах мониторинга ACRC (SOC) использует собственную модель «Cyber-Kill Chain», которая является упрощенной моделью MITRE, адаптированной на основе опыта аналитиков Центра киберустойчивости для организаций на территории РФ. Процессы мониторинга выстроены таким образом, чтобы максимально повысить вероятность выявления атак на ранних стадиях. Приведем относительное распределение подтвержденных Инцидентов по стадиям модели:

Большая часть подтвержденных Инцидентов пришлась на стадии «Эксплуатация» и «Заражение». Это связано с невозможностью определения некоторых Инцидентов на более ранних стадиях: заражение осуществляется через съемные носители, или у аналитиков отсутствует информация, позволяющая выявить вредоносную активность на более ранних стадиях, например, при использовании BYOD или корпоративных мобильных устройств за пределами периметра без осуществления контроля доступа в Интернет. Также, около 8% Инцидентов пришлось на ошибки конфигурации и 4% – на Инциденты, связанные с некорректно настроенными политиками безопасности наших Клиентов.

5 Управление правилами автоматизированного выявления

В связи с постоянно меняющимся профилем выявляемых Инцидентов, необходим регулярный пересмотр и актуализация существующих правил. Наши Клиенты проявляют большой интерес к новым правилам, разрабатываемым на основе метода «Hunting». Однако аналитики ACRC стараются уделять не меньше внимания адаптации и тюнингу уже имеющихся правил: списки исключений, значения важности и достоверности, пороги срабатывания – для поддержания уровня эффективности выявления угроз. Все это необходимо постоянно актуализировать и перенастраивать под динамично меняющиеся различные информационные инфраструктуры наших Клиентов. Нередко временно отключенные правила или правила с очень высоким порогом срабатывания (правила с низкой достоверностью) вводятся в действие и перенастраиваются несмотря на последствия: существенный рост ложноположительных срабатываний. Этого требует постоянно изменяющиеся вектора вредоносной активности, ведь злоумышленники не редко пользуются правилом «новое – это хорошо забытое старое».

Цикл разработки и пересмотра правил выявления угроз нашего Центра киберустойчивости можно представить следующим образом:



Аналитиками проводится постоянная оптимизация базы правил с целью покрытия актуальных для наших Клиентов тактик и техник согласно матрице MITRE. Обновление правил в ACRC происходит в формате спринтов и разбито на следующие этапы:

1) Проверка, по каким тактикам и техникам правила отсутствуют. Эта информация задает вектор по развитию правил на спринт.
2) Выявление самых неэффективных правил. Для выявления таких правил используется статистика ACRC. Если правило выдает ложное срабатывание в более, чем 90% случаев, то оно подлежит пересмотру.
3) Проверка исключений, которые вносились в то или иное правило. При начальной эксплуатации некоторые правила только кажутся полезными и требуют постоянного внесения исключений для отсеивания легитимной активности. В ходе спринта происходит оптимизация правил с целью оптимизации количества исключений.
4) Разработка новых правил, которые формируются на основе предположений аналитика о возможных действиях злоумышленника в информационных инфраструктурах наших Клиентов.
5) По результатам всех работ формируется новый пакет, содержащий правила для предварительного тестирования.
6) В случае если во время тестирования выявлены недостатки в правилах, они возвращаются на доработку, после которой снова возвращаются на тестирование.
7) Когда пакет правил сформирован и протестирован – производится централизованное обновление правил у клиентов, если в их инфраструктуре имеются необходимые для работы правил источники событий.

Например, в последнем спринте были доработаны правила, генерирующие большой поток ложных срабатываний. К таким правилам относятся общие правила, выявляющие подозрительную активность на хостах: запуск подозрительных процессов по различным критериям, выполнение команд, свойственных разведывательной деятельности злоумышленников, добавление исполняемых файлов в автозагрузку и многое другое. Данные правила были доработаны или декомпозированы для удобства внесения исключений, прошли тестирование на нашей инфраструктуре и уже внедрены у некоторых наших Клиентов.

Заключение

В первой половине года мир столкнулся с новыми вызовами. Приспосабливаться в сжатые сроки пришлось всем, в частности, коммерческим поставщикам услуг SOC. Центру киберустойчивости и нашим Клиентам удалось адаптироваться к текущей ситуации за короткое время и, хотя и произошел общий рост вредоносной активности, она не отразилась на функционировании бизнеса наших Клиентов.

О группе компаний Angara

Группа компаний Angara представлена системным интегратором Angara Technologies Group и сервис-провайдером Angara Professional Assistance и оказывает полный спектр услуг по информационной безопасности: поставку оборудования и ПО, проектирование, внедрение, сопровождение систем ИТ и ИБ клиентов, а также предлагает сервисы по обеспечению информационной безопасности по модели подписки.

Группа компаний входит в:

- ТОП-10 самых быстрорастущих ИТ-компаний России (7 место, CNews);
- ТОП-20 крупнейших компаний информационной безопасности (12 место, TAdviser);
- ТОП-20 крупнейших поставщиков для банков (19 место, TAdviser);
- ТОП-100 крупнейших ИТ-компаний России по версии CNews и TAdviser.

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.

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

Истории успеха

Компания	Проект
СПАО «Ингосстрах»	«Ингосстрах» и группа компаний Angara создают центр мониторинга информационной безопасности
ООО «ИНБАНК»	Оказание услуг по мониторингу ИБ (SOC)
Банк «Юнистрим»	Оказанию услуг по выявлению и реагированию на инциденты ИБ
АО «ЭР-Телеком Холдинг»	Создание системы сбора и визуализации событий ИБ
Банк «Санкт-Петербург»	Трансформация центра мониторинга ИБ (SOC)

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).

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.

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

2020 г.