ANGARA
professional assistance

ACRC
ANGARA CYBER RESILIENCE CENTER

ОТЧЕТ ACRC 2020

ANGARA PROFESSIONAL ASSISTANCE
ЦЕНТР КИБЕРУСТОЙЧИВОСТИ
ANGARA CYBER RESILIENCE CENTER

ANGARAPRO.RU

ОГЛАВЛЕНИЕ

01 О нас 3

02 Сводная статистика 6

03 Нестандартные инциденты 10

Natворил 10

Вовремя разобрали 11

UnNinvoke Obfuscation 12

04 Ключевые нововведения в нашем SOC 13

05 Новая услуга 15

06 О группе компаний Angara 16

ОГЛАВЛЕНИЕ

01 О нас 3

02 Сводная статистика 6

03 Нестандартные инциденты 10

Natворил 10

Вовремя разобрали 11

UnNinvoke Obfuscation 12

04 Ключевые нововведения в нашем SOC 13

05 Новая услуга 15

06 О группе компаний Angara 16

01_ О НАС

Данный отчет сформирован с использованием данных коммерческого SOC - Angara Cyber Resilience Center (ACRC), работающего в рамках Центра киберустойчивости группы компаний Angara.

Эксперты группы компаний Angara из подразделений Центра киберустойчивости - отдела систем мониторинга и реагирования **(ОСМР) и ACRC**, отвечают за реализацию проектов по внедрению и развитию решений класса SIEM, SGRC, IRP/SOAR, Threat Intelligence & Security Feeds и Security Intelligence, предоставляют услуги коммерческого SOC, активно участвуют в жизни российского и международного сообщества ИБ (OSCD), осуществляют вклад в развитие открытых репозиториев со Сценариями детектирования угроз (Sigma (@zinin и др.)), публикуют работы на открытых тематических ресурсах (habr (@ANosarev) & SecurityLab (@MPavlunin)) и помогают в переводе работ зарубежных авторов на русский язык (habr (@zinint)).

Все это выполняется с целью предоставления современных экспертных решений для следующих задач наших заказчиков:

- Коммерческий SOC - ACRC с возможностью подключения к ГосСОПКА.
- Автоматизация процессов ИБ в части организации мониторинга событий (SIEM/SEM).
- Обогащение процессов ИБ сторонней аналитикой (TI(P) & Security Feeds).
- Мониторинг и управление инцидентами ИБ (SIEM/IR(P)) [On-Premise & Outsource].
- Автоматизация управления и реагирования на инциденты ИБ (IR(P)/SOAR) [On-Premise & Outsource].
- Визуализация и контроль метрик эффективности СЗИ (SI).

На момент создания отчета под защитой ACRC находится:

более **10** организаций коммерческого сектора.

ОСМР оказывает услуги:

более чем **30** различным организациям, включая крупные федеральные ведомства.

ACRC, являясь участником информационного обмена о киберугрозах, активно взаимодействует с **ФинЦЕРТ ЦБ РФ,** а в рамках статуса **Корпоративного Центра ГосСОПКА Класса А** – с **ГосСОПКА ФСБ РФ.**

Подразделения Центра киберустойчивости группы компаний Angara расположены в Москве и Рязани, где руководитель Центра мониторинга ACRC преподает студентам старшего курса одного из государственных технических вузов практический авторский курс для аналитиков SOC.

Текущий штат сотрудников Центра киберустойчивости группы компаний Angara насчитывает более

30 человек.

Сертификаты соответствия системы менеджмента качества и системы менеджмента ИБ

Свидетельство №2018660748 о государственной регистрации ПО

Зарегестрированный участник информационного обмена Финцерт

Данные для отчета представляют собой результаты анализа инцидентов ИБ, выявленных ACRC в ходе оказания услуг коммерческого SOC.

Используемая в отчете классификация инцидентов основана на модели Cyber Kill Chain собственной разработки, состоящей из 7 стадий атаки и 2 вспомогательных стадий, характеризующих непреднамеренные действия, которые могут иметь негативные последствия и повлечь нарушения политик ИБ наших клиентов.

- РАЗВЕДКА
- ДОСТАВКА
- ЭКСПЛУАТАЦИЯ
- ЗАРАЖЕНИЕ
- ЗАКРЕПЛЕНИЕ
- ДОСТИЖЕНИЕ ЦЕЛЕЙ
- УНИЧТОЖЕНИЕ СЛЕДОВ
- ОШИБКА КОНФИГУРАЦИИ
- НАРУШЕНИЕ ПОЛИТИКИ ИБ

Каждой стадии Cyber Kill Chain ACRC соответствует определенный набор правил ACRC – детектирующих инструкций, направленных на выявление признаков потенциальной злонамеренной активности, например «Использование утилит из пакета PsTools». Для облегчения интеграции в процессы наших клиентов правила по модели Cyber Kill Chain ACRC были классифицированы в соответствии с матрицей MITRE ATT&CK®.

02_ СВОДНАЯ СТАТИСТИКА

99.85%

составило среднее значение обязательства по ключевому показателю доступности соглашения об уровне услуг (SLA) с нашими клиентами.

~2,1 млрд событий

составил среднесуточный поток событий ИБ, поступающих после фильтрации в инсталляции ACRC, используемые для оказания услуг.

Этот прирост в сравнении с показателями I полугодия 2020 года связан с подключением новых клиентов.

~2060

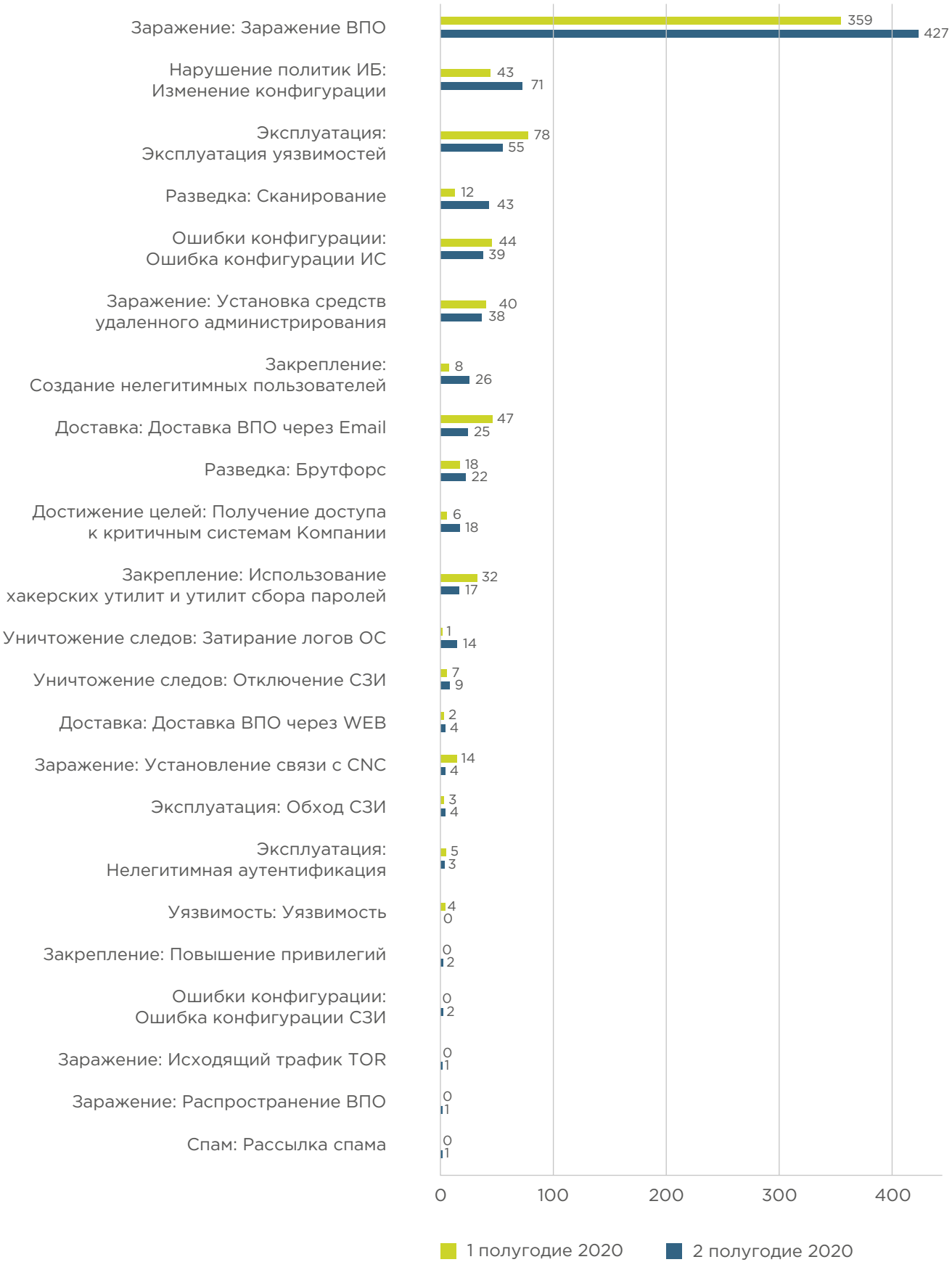
Gb в день (raw) составил среднесуточный объем событий, обрабатываемых ACRC.

Всего за 2020 год ACRC было зафиксировано 19 482 подозрений на инциденты ИБ.

Во II полугодии 2020 года количество регистрируемых подозрений выросло по сравнению с началом года, а пиковая активность пришлась на два последних месяца в году. Относительные цифры за год по части* подтвержденных инцидентов ИБ в динамике можно представить следующим образом (легенда графика представлена в формате [стадия атаки: наименование правила], согласно Cyber Kill Chain ACRC):

*часть данных не публикуется в связи с ограничением возможности публикации данной информации в открытых источниках

КОЛИЧЕСТВО ПОДТВЕРЖДЕННЫХ ИНЦИДЕНТОВ ЗА 2020 ГОД

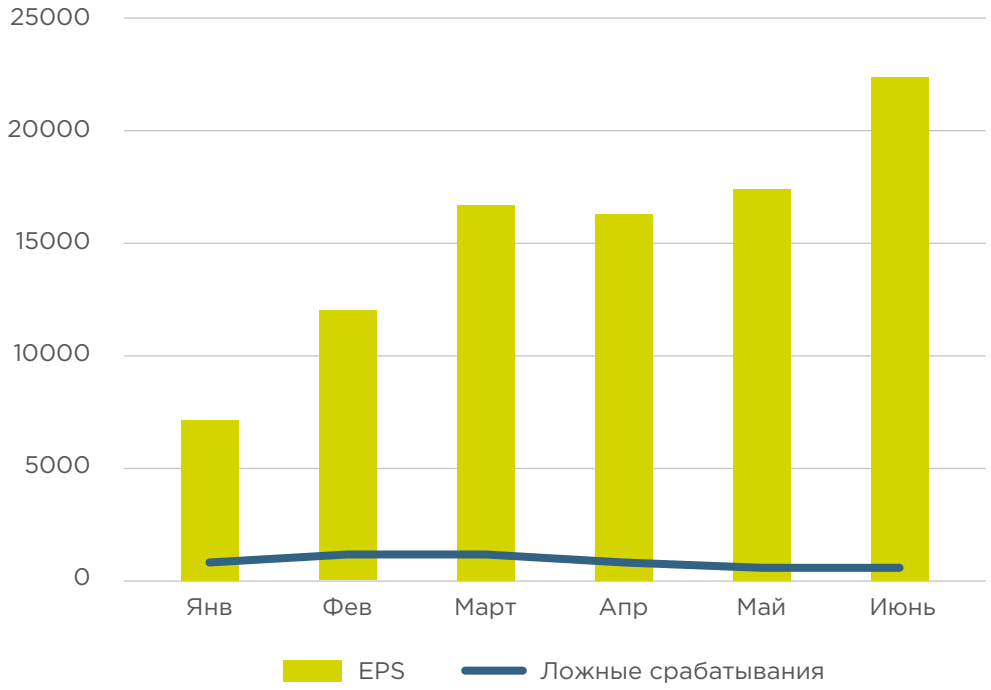


РАСПРЕДЕЛЕНИЕ ПОДТВЕРЖДЕННЫХ ИНЦИДЕНТОВ СОГЛАСНО МОДЕЛИ CYBER KILL CHAIN ACRC ВО ВТОРОМ ПОЛУГОДИИ:

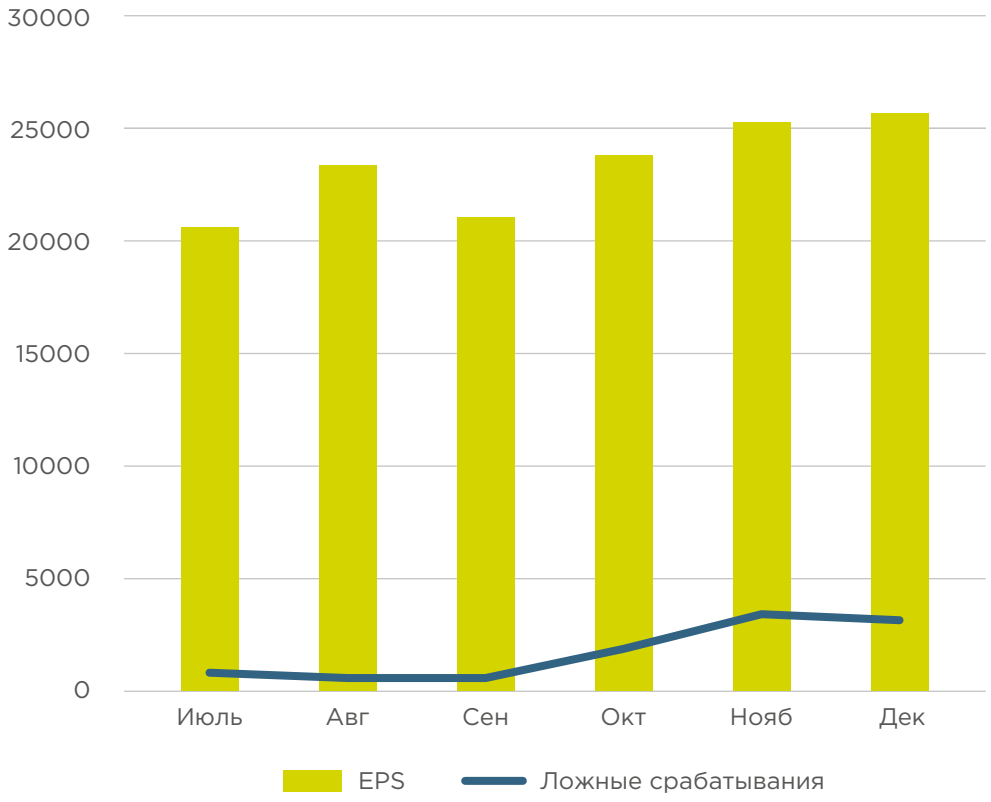
- Заражение: Заражение ВПО
- Нарушение политик ИБ: Изменение конфигурации
- Эксплуатация: Эксплуатация уязвимостей
- Разведка: Сканирование
- Ошибки конфигурации: Ошибка конфигурации ИС
- Заражение: Установка средств удаленного администрирования
- Закрепление: Создание нелегитимных пользователей
- Доставка: Доставка ВПО через Email
- Разведка: Брутфорс
- Достижение целей: Получение доступа к критичным системам Компании
- Закрепление: Использование хакерских утилит и утилит сбора паролей
- Уничтожение следов: Затирание логов ОС
- Уничтожение следов: Отключение СЗИ
- Доставка: Доставка ВПО через WEB
- Заражение: Установление связи с CNC
- Эксплуатация: Обход СЗИ
- Эксплуатация: Нелегитимная аутентификация
- Закрепление: Повышение привилегий
- Ошибки конфигурации: Ошибка конфигурации СЗИ
- Заражение: Исходящий трафик TOR
- Заражение: Распространение ВПО
- Спам: Рассылка спама
- Уязвимость: Уязвимость

КОЛИЧЕСТВО ЛОЖНЫХ СРАБАТЫВАНИЙ НА ОБЩЕМ ПОТОКЕ СОБЫТИЙ В УШЕДШЕМ ГОДУ:

Соотношение FPR к общему потоку событий за 1-ое полугодие 2020 года



Соотношение FPR к общему потоку событий за 2-ое полугодие 2020 года



03_ НЕСТАНДАРТНЫЕ ИНЦИДЕНТЫ

NATВОРИЛ

В рамках расследования одного из инцидентов ИБ, в котором фигурировал пользователь, работавший удаленно с использованием корпоративного ПК, было выявлено, что из-за неправильной конфигурации домашней сети пользователя оказалась возможна работа хоста с белым адресом сети Интернет без NAT.

В результате чего порты ОС Windows корпоративного ПК (в частности 445\tcp) оказались доступны в сети Интернет, чем и воспользовались злоумышленники для развития атаки.

!!! О ХОДЕ РАССЛЕДОВАНИЯ:

На одном из корпоративных ПК агентом ACRC были зафиксированы множественные срабатывания endpoint IPS по различным сигнатурам, связанным с эксплуатацией уязвимостей протокола SMB. Но в качестве IP-адреса ПК был указан внешний адрес сети Интернет, который принадлежит одному провайдеру услуг в Московской области. В случае успешной атаки, злоумышленник с применением средств Pivoting мог получить прямой доступ к корпоративной инфраструктуре, т.к. удаленный пользователь был подключен к корпоративной сети через VPN.

!!! РЕКОМЕНДАЦИИ ACRC:

Необходимо всегда следовать указаниям производителя Вашего домашнего сетевого оборудования по безопасной конфигурации устройства или запрашивать их у своих коллег из подразделения информационной безопасности. На корпоративных ПК для домашнего использования желательно наличие endpoint агентов с функциями МСЭ и IPS или же обязательный произведенный хардеринг встроенных средств ОС.

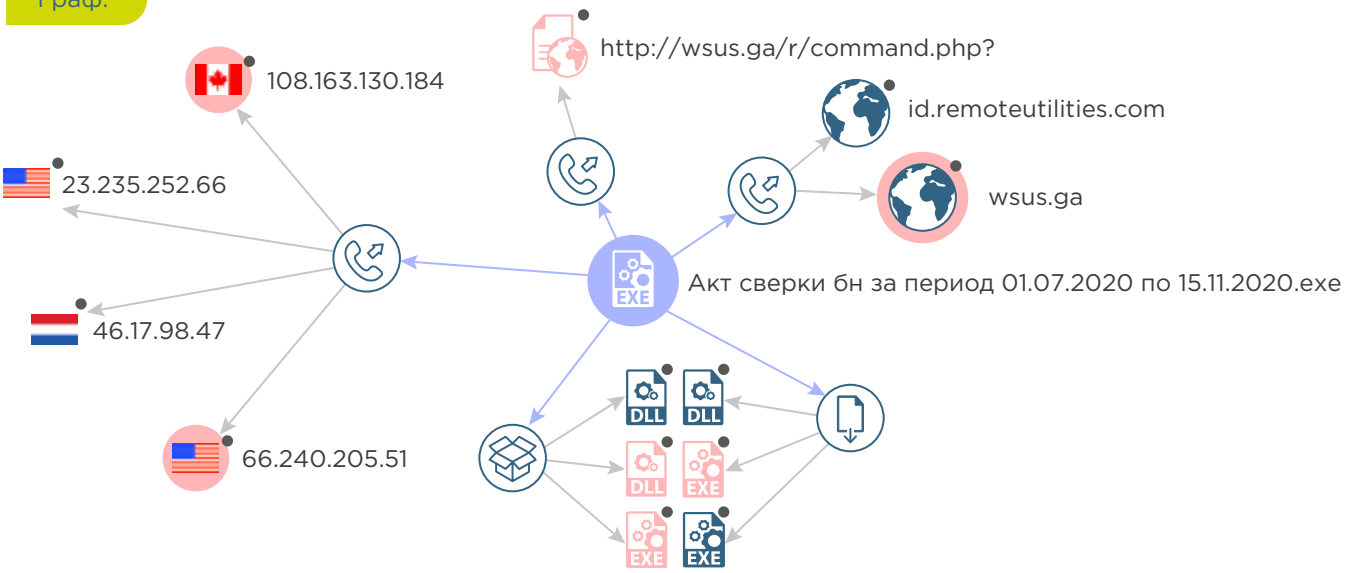
В ходе фишинговой почтовой рассылки сотрудникам организации доставлялось ВПО под видом типовых распорядительных документов, часто использующихся в соответствующем виде деятельности.

В ходе анализа инцидента удалось оперативно получить образец ВПО и установить внутреннюю и внешнюю активность посредством песочницы. Собранные индикаторы компрометации позволили выявить и устранить заражение других пользователей клиента. Спустя несколько часов после устранения инцидента аналогичные индикаторы были опубликованы в бюллетенях ФинЦЕРТ ЦБ РФ:

Имя файла: «Акт сверки бн за период 01.07.2020 по 15.11.2020.exe»

Контрольная сумма SHA-256: ac44cee7b064d2ef26af281a67129a29562da3b0dd763782855ab38328e01985

Граф:



!!! О ХОДЕ РАССЛЕДОВАНИЯ:

На одном из корпоративных ПК клиента агентом ACRC был выявлен запуск подозрительного исполняемого файла. В ходе анализа активности созданного им процесса был выявлен ряд типичных для ВПО признаков поведения. В рамках расследования было установлено, что исходный файл пришел нескольким пользователям в электронном письме от недоверенного источника, после чего службе ИБ клиента были направлены рекомендации для удаления вредоносных писем и устранения заражения на хостах, где имелись признаки запуска аналогичных исполняемых файлов. После получения образца ВПО были установлены все индикаторы компрометации, которые были незамедлительно применены для дополнительной проверки с целью определения потенциально невыявленных, скомпрометированных ПК.

UNINVOKE OBFUSCATION

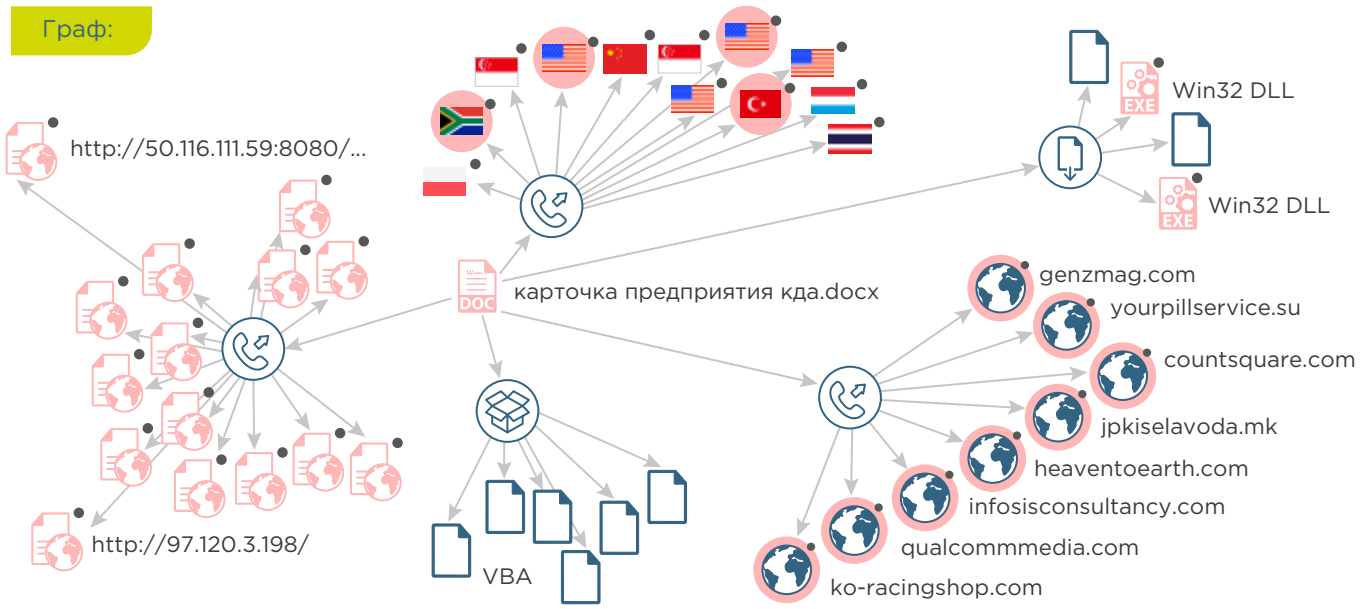
Было зарегистрировано подозрение на инцидент, связанное с запуском обфусцированных скриптов от процесса MS Word.

Документ с полезной нагрузкой был получен по электронной почте от недоверенного источника под видом легитимного юридического документа, что не вызвало подозрений у пользователя. В ходе расследования нашим аналитикам удалось деобфусцировать запускаемые скрипты и установить все внешние ресурсы, с которых осуществлялась попытка запуска вредоносного кода. Все индикаторы компрометации были вовремя переданы подразделению ИБ клиента для блокировки на СЗИ.

Имя файла: «карточка предприятия кда.docx»

Контрольная сумма SHA-256: 9720a3e0e322e5daf89a2d48916ae17a8d58eadcf34fdbddd7955ecf2d7007e8

Граф:



!!! О ХОДЕ РАССЛЕДОВАНИЯ:

В данном случае интересен был именно способ обфускации, т.к. применялось сразу несколько обфусцирующих методов, что затрудняло извлечение индикаторов компрометации. После успешной деобфускации всех наложенных методов удалось извлечь и передать службе ИБ клиента индикаторы компрометации для блокировки всех внешних ресурсов, откуда предполагалось скачивание и запуск вредоносной полезной нагрузки.

!!! РЕКОМЕНДАЦИИ ACRC:

«Согласно статистике CISA, а именно Anti-Phishing Working Group (APWG), количество фишинговых рассылок за ушедший год выросло **более чем в два раза. Более 3/4 всех атак** по различным отчетам начинаются именно с фишинга. Будьте внимательны, не теряйте бдительность. Всегда лучше лишний раз отправить подозрительное письмо коллегам из подразделения информационной безопасности для проверки перед тем, как открыть подозрительные ссылки или вложения, даже от известных Вам отправителей!».

04_ КЛЮЧЕВЫЕ НОВООВВЕДЕНИЯ В НАШЕМ SOC

PURPLE TEAM

В связи с объединением отдела систем мониторинга и реагирования интегратора Angara Technologies Group с подразделениями Angara Cyber Resilience Center в единый Центр киберустойчивости группы компаний Angara, а также сопутствующим расширением дорожной карты используемых ресурсов, у ACRC появилась возможность проведения киберучений (спринтов) с Red Team (интеллектуальная база – эксперты отдела анализа защищенности Angara Technologies Group).

Целями проведения киберучений являются:

01_ Тренировка сотрудников SOC и Red Team.

02_ Проверка работы линий ACRC в боевых условиях.

03_ Проверка работы подсистемы автоматизированного выявления инцидентов собственной разработки ACRC и правил в боевых условиях.

04_ Развитие алгоритмов детектирования и расследования инцидентов ИБ.

05_ Выявление слабых мест в тактиках, техниках и инструментах SOC и Red Team с целью последующего совершенствования.

06_ Работа над ошибками.

В ходе учений команда Red Team осуществляет ряд атак, направленных на боевую информационную инфраструктуру группы компаний Angara. Команда аналитиков SOC при этом не предупреждается и в боевых условиях осуществляет расследование подозрений на инциденты ИБ и выявление данных атак.

После завершения киберучений команды обмениваются отчетами о результатах работ, определяют слабые места в тактиках, техниках и инструментах защиты и нападения, составляют план мероприятий по развитию и/или корректировке используемых средств и назначают ответственных за задачи согласно плану. По факту назначения ответственных лидеры команд приступают к планированию даты начала подготовки следующего спринта (согласно применяемым в группе компаний Angara принципам PDAR).

Результаты проделанных работ немедленно включаются в план обновлений, используемых ACRC инструментов, у наших клиентов.

Нормативной базой для планирования спринтов преимущественно должны выступать следующие стандарты и рекомендации, включая, но не ограничиваясь:

Singapore – AASE (2018)

EU - TIBER-EU (2018)

NATO – Cyber Red Teaming (2015)

UK – CBEST (2016)

05_ НОВАЯ УСЛУГА

ПРОВЕРКА СТОЙКОСТИ ПАРОЛЕЙ

Благодаря уже упомянутому объединению, ACRC включает в состав своих услуг уникальную услугу по автоматизированной проверке стойкости паролей.

ОСНОВНЫЕ ЦЕЛИ НОВОЙ УСЛУГИ:

Выявление слабых, легкоугадываемых паролей, используемых в корпоративных учетных записях домена Active Directory клиента, выявление паролей, содержащихся в общедоступных и частных базах утечек данных аутентификации публичных ресурсов, формирование перечня учетных записей, содержащих нестойкие пароли, выработка рекомендаций по генерации стойких к перебору паролей.

В результате приобретения данной услуги планово на периодической основе будут выявляться пароли, которые возможно подобрать за ограниченное количество времени при применении техники Password Spraying (T1110.003 согласно классификации MITRE ATT&CK®).

06_ О ГРУППЕ КОМПАНИЙ ANGARA

Группа компаний Angara представленная системным интегратором Angara Technologies Group и сервис-провайдером тиражируемых услуг безопасности Angara Professional Assistance, оказывает полный спектр услуг по информационной безопасности, начиная с поставки и внедрения оборудования и ПО, заканчивая комплексом мероприятий по сопровождению ИТ- и ИБ-систем клиентов.

ГРУППА КОМПАНИЙ ВХОДИТ В:

- ТОП-30 крупнейших компаний информационной безопасности (TAdviser);
- ТОП-30 крупнейших компаний России в сфере защиты информации (CNews);
- ТОП-50 крупнейших поставщиков ИТ-решений для госсектора (CNews);
- ТОП-50 крупнейших поставщиков ИТ-услуг (TAdviser);
- ТОП-50 крупнейших поставщиков ИТ для финансового сектора (CNews);
- ТОП-100 крупнейших ИТ-компаний России (TAdviser);
- ТОП-100 крупнейших ИТ-компаний России (CNews).

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)

более

50 экспертов

насчитывает команда Angara Professional Assistance 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
- Отчет Центра киберустойчивости Angara Cyber Resilience Center (ACRC) за I полугодие 2020 года

ANGARA
professional assistance

ACRC
ANGARACYBER RESILIENCE CENTER

121096, Г. МОСКВА,
УЛ. ВАСИЛИСЫ КОЖИНОЙ, Д.1, КВ.1
БЦ «ПАРК ПОБЕДЫ»
ТЕЛ.: +7 (495) 269 26 07
EMAIL: INFO@ANGARAPRO.RU