Победа на PHDays 9. Делимся лайфхаками в трёх частях. Часть 2

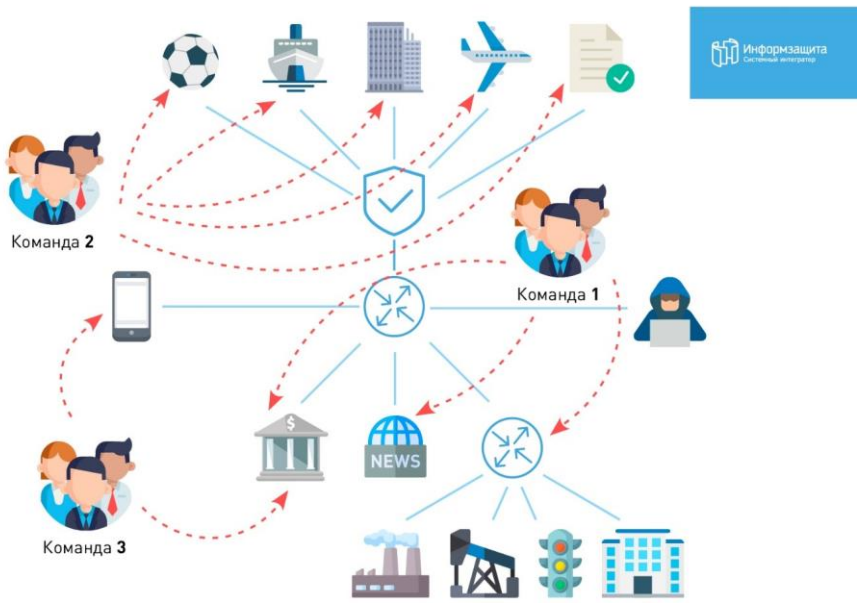
Издание: Хабр, 3 июня 2019 г.

Спикер: Виталий Малкин, руководитель отдела анализа защищенности «Информзащиты»

Всем привет! Меня зовут Виталий Малкин. Я руководитель отдела анализа защищённости компании «Информзащита» и по совместительству капитан команды True0xA3. Чуть больше недели назад мы победили в одном из самых престижных соревнований белых хакеров в СНГ. В прошлой статье (если вы пропустили её, можно почитать тут) мы рассказали о важности предварительной подготовки. В этой — я расскажу о том, что происходило непосредственно на самих соревнованиях, объясню почему иногда важно вносить коррективы в уже существующие планы по ходу игры и почему, на мой взгляд, ни один из защищаемых офисов не был взломан.

День первый

9:45 MSK
День начался с того, что нам раздали результаты запуска MassScan-а. Мы стартовали с того, что сразу выписали все хосты с открытым 445 портом и ровно в 10.00 запустили уже готовый чекер метасплойта на предмет MS17-010. Руководствуясь нашим планом, задачей №1 было захватить домен bigbrogroup, поэтому его одновременно ломали сразу два человека из нашей команды. На схеме ниже вы можете увидеть первичное распределение членов нашей команды по офисам.



Как видно из схемы, нами были охвачены практически все офисы. И здесь очень помог тот факт, что в команде нас было 20 человек.

10:15
К этому времени один из членов Команды-1 находит в bigbrogroup.phd хост, уязвимый к MS17-010. Мы проэксплуатировали уязвимость в невероятной спешке.

Несколько лет назад мы уже были в ситуации, когда получили meterpreter shell к важному узлу и через 10 секунд нас выкинули с него, попутно закрыв порт. В этом году такого не произошло: мы успешно захватываем узел, закрываем SMB-порт и меняем порт RDP на 50002. Мы очень ответственно относимся к вопросу сохранения доступа, поэтому добавляем ещё несколько локальных администраторов и устанавливаем свой собственный RAT. После этого двигаемся дальше.

10:25
Мы продолжаем разбираться с тем, что нашли. Помимо того, что у этого узла есть доступ во внутреннюю сеть и к домен-контроллеру, на нём также обнаруживается токен администратора домена. Это джэкпот! Мы тут же проверяем, не «протух» ли он, и нашей радости нет предела. Первый домен пал. Время взлома — 27 минут 52 секунды.

Наконец-то спустя полчаса с момента начала соревнований мы таки заходим в портал хакеров и пытаемся понять, а что же нам надо сделать, чтобы получить публи. Видим стандартный набор: учётные данные администратора домена, администратора рабочих станций, exchange, а также нескольких топов. Мы скачиваем с домена ntds.dit, попутно расчехляя CUDA-станцию. Каково же было наше удивление, когда мы увидели, что в домене включен режим обратимого шифрования, позволяющий нам получить все пароли пользователей в открытом виде. Чтобы сформировать понимание, какие пользователи нам интересны — задействовали двух человек из Команды-1 для анализа структуры AD и её групп. Через пять минут у нас появились все ответы. Мы отправляем их на портал и начинаем ждать. Честно — уже к тому времени очень хотелось пролить первую кровь для поддержания морального духа так сказать, но лишь спустя час мы смогли понять как работает чекер:

а) чекер автоматизирован;
б) у чекера есть жёсткий формат;
в) чекер через несколько секунд после отправки ответа не принял наш ответ, т.к. он был в неправильном формате.

Совладав с форматом, примерно в 11.00 мы получаем заветный First blood. Eeeee!

11:15
Команду-1 разделяем на две части. Участники одной подкоманды продолжают закрепляться в домене: получают krbtgt, укрепляют домен, меняют пароли для учётных записей. Организаторы PHDays ещё на брифинге чётко дали понять — кто первый встал, того и тапки. Поэтому мы меняем пароли на учётных записях, чтобы быть уверенными: если нас кто-то выкинет, они получат минимум баллов.

Команда-2 при этом продолжает исследовать домен, и находит ответ ещё к одному заданию. На рабочем столе финансового директора обнаружен финансовый отчет, так необходимый кому-то. Но вот беда — он в архиве, который запаролен. Ну что ж, не зря мы расчехляли CUDA-станцию. Лёгким движением руки превращаем архив в хэш и отправляем его в hashcat.

Команда-2 в это время находит несколько интересных сервисов с RCE и начинает их «крутить». Это мониторинг в CF-media, построенный на основе Nagios. Это система рисования графиков из корабельной компании, построенная на технологии, которую видим впервые. А также ещё несколько потенциально интересных сервисов типа конвертера из DOC в PDF.

Вторая подкоманда Команды-1 тем временем занимается банком и находит интересную базу на MongoDB, в которой, в том числе, есть название нашей команды и её баланс в какой-то системе. «Подкручиваем» наш баланс на 50 млн и идём дальше.

14:00
Нас настигают первые неудачи. Во-первых, два сервиса, на которых мы получили RCE в защищаемых сегментах, стали недоступны. Защитники их просто отключили. Разумеется идём жаловаться к организаторам. Это ни к чему не приводит. Ну да, в Standoff увы нет бизнеса, которые надавали бы за такое по шапке. Помимо этого, мы никак не можем найти список клиентов. Предполагаем, что он запрятан где-то в глубинах 1С, но нет ни баз, ни рабочих конфигураций. Это тупик.

Мы пытаемся поднять VPN-канал между нашими удаленными серверами и сетью АСУ ТП. По непонятным причинам делаем это на домен-контроллере bigbrogroup, и в момент построения моста между интерфейсами соединение обрывается. Домен-контроллер недоступен. У части команды, которая захватила bigbrogroup, чуть было не случился инфаркт: начинаются первые ссоры, всеобщее напряжение нарастает.

Неожиданно мы понимаем, что домен-контроллер всё ещё доступен с наших серверов, но канал очень нестабилен. Как в пошаговой стратегии — мы через RDP отключаем режим моста, домен-контроллер снова доступен. Фух!!! Все успокаиваются. VPN мы в итоге поднимаем с другого сервера, домен-контроллер холим и лелеем. У всех команд по нулям баллов, это успокаивает.

16:50
Организаторы наконец-то публикуют майнер и мы, используя psexec, устанавливаем его на всех подконтрольных нам узлах. Получаем дополнительный стабильный доход.

Команда-2 докручивает уязвимость Nagios. Там установлена уязвимая версия <=5.5.6 CVE-2018-15710 CVE-2018-15708. Публичный эксплойт существует, но использует Reverse-коннект для скачивания web-шелла. Мы за NAT-ом, поэтому приходится переписать эксплойт и разбить его на две части. Первая заставляет Nagios подключиться к нашему удалённому серверу через Интернет, а вторая, находящаяся непосредственно на сервере, отдает Nagios-у web-шелл. После получения web-шелла был загружен WSO и удален уязвимый PHP-скрипт «magpie_debug.php». Это даёт нам доступ через прокси к домену CF-media. Подключение нестабильно и использовать его тяжело, решаем отправить эксплойт на Bug-bounty, а сами в это время пытаемся «повыситься» до Root.

18:07
А вот и обещанные сюрпризы от организаторов: BigBroGroup покупают CF-media! В целом мы предполагали подобный поворот. В ходе исследования домен-контроллера bigbrogroup мы заметили доверие между этим доменом и доменом cf-media.

К сожалению, на тот момент сетевого доступа не было. Но в момент объявления о слиянии он появился. Это избавило нас от головной боли, связанной с пивотингом через nagios. Учётные данные bigbrogroup работают на cf-media, но пользователи непривилегированны. Легко эксплуатируемых уязвимостей нет, но мы не отчаиваемся. Что-то быть должно.

18:30
Нас выбивают с домен контроллера BigBroGroup. Кто? Где? Похоже, что команда ЦАРКА. Они меняют пароль доменного администратора, но у нас четыре резервных. Меняем обратно, сбрасываем все пароли. Не помогает, нас снова выбивают.

В это же время мы находим вектора в CF-media. На одном из серверов используется тот же пароль локального администратора, что и в домене bigbrogroup. Ну что же, password reuse, осталось подобрать хэш! Используя hashkiller находим пароль — «P@ssw0rd». Ломимся дальше.

19:00
Сражение за bigbrogroup не останавливается. ЦАРКА меняет дважды пароль на krbtgt, мы потеряли всех админов. Это конец?

19:30
Получаем домен администратора CF-media, начинаем сдавать флаги. Несмотря на то, что домен вроде как должен быть настроен максимально безопасно, опять включено обратное шифрование. Получаем явки, логины, пароли. Повторяем всё как и в прошлом домене: закрепляемся, харденим, меняем пароли, прокидываем VPN. Находим второй финансовый отчет. Кстати, что там с первым? Первый уже сбрутился, но не принимается оргами. Оказывается, сдавать нужно зашифрованный 7z!!! Брутить ничего не нужно было, три часа насмарку!!!

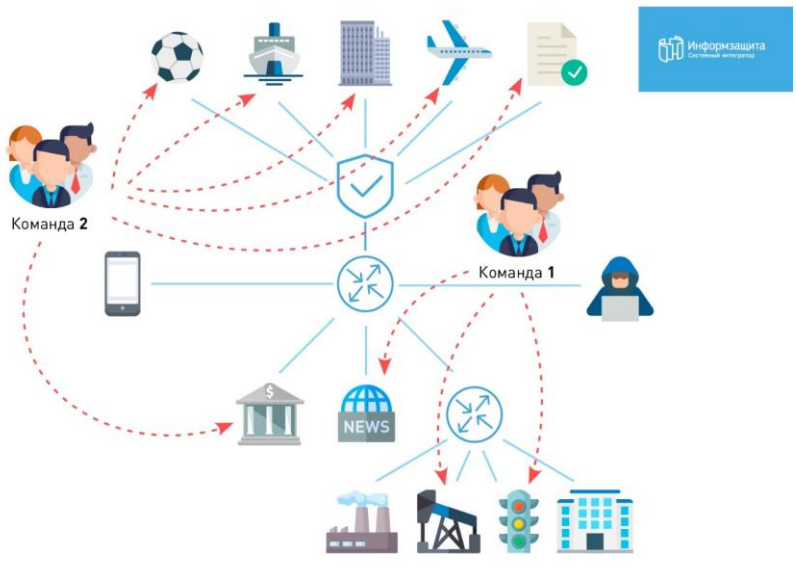
В итоге сдаем оба. У нас около 1млн баллов, у ЦАРКА 125.000, остальные по нулям. ЦАРКА начинает сдавать флаги с Bigbrogroup. Мы понимаем, что это нужно срочно остановить, но КАК?!

19:45
Появилось решение!!! У нас остались учётные данные локальных администраторов. Подключаемся, забираем ticket и решаем просто уронить домен. Домен отправляется в power off, закрываем все порты на серверах, кроме RDP, меняем пароли локальных администраторов. Теперь мы сами по себе, и они сами по себе. Еще бы добиться стабильной работы VPN и всё вообще было бы отлично. Выыыдохнули…

Раскидываем miner по всем узлам в домене CF-media. ЦАРКА нас обгоняет по общему объёму, но мы явно догоняем их, ведь мощности у нас побольше.

Ночь

На картинке вы можете наблюдать распределение команды ночью.



Ребята постепенно начинают расходиться по домам. К полуночи нас остается девять человек. Эффективность очень сильно снижается. Каждый час мы отлучаемся умыться и подышать — чтобы не уснуть.

Приступаем к АСУ ТП.

02:00
Ночь выдается очень тяжелой. Мы несколько раз находим вектора, но они уже закрыты. Не совсем понятно, были ли они изначально закрыты, или до нас тут уже побывала ЦАРКА и закрыла их. Постепенно осваиваясь в АСУ ТП, находим уязвимый к атаке через NetBus контроллер. Используя модуль метасплойта, делаем что-то, не до конца понимая что. Свет в городе тухнет. Организаторы готовы засчитать задание, если мы сможем включить свет обратно. В этот момент снова падает VPN-соединение. Сервер, на котором развернут VPN, находится под контролем ЦАРКи. Снова кажется, что это конец: мы слишком шумно обсуждали АСУ ТП и они смогли как-то нас отключить.

03:30
Самых стойких «рубит» сон. Бодрствующих остается всего семеро. Неожиданно (без видимых причин) VPN начинает снова работать. Мы быстро повторяем фокус со светом. Есть +200.000 публей!!!

Часть команды продолжает искать другие вектора, часть продолжает активно работать с АСУ ТП. Мы находим еще две потенциальных уязвимости. Одну из них нам удается проэксплуатировать. Результатом может стать перезапись прошивки контроллера. Договариваемся с организаторами, что подождем до утра и вместе решим, что делать.

05:30
VPN работает 10 минут в час, в остальное время он отмирает. Мы пытаемся найти хоть что-нибудь. Наша производительность практически на нуле. Решаем поспать хотя бы по часику. СПОЙЛЕР: плохая идея.

Пять ребят продолжают ломать АСУ ТП.

Утро

К утру мы понимаем, что существенно оторвались по баллам от остальных, почти на 1 млн. ЦАРКА смогла сдать два задания из АСУ ТП и несколько заданий из телекома и bigbrogroup. Они уже немало намайнили, но по нашим подсчетам у них есть запас, который они еще не продали. По текущему курсу он выходил на 200-300 т. публей. Нас это пугает: появляется ощущение, что у них в загашнике может быть еще несколько флагов, которые они могут приберечь для финального рывка. В нашем полку прибывает. Утренний саунд-чек на площадке немного раздражает, но бодрит.

Мы все так же пытаемся сломать АСУ ТП, но без особых надежд. Разрыв между командами, претендующими на первое и второе место, и остальными — слишком велик. Мы не верим, что организаторы оставят все так как есть.

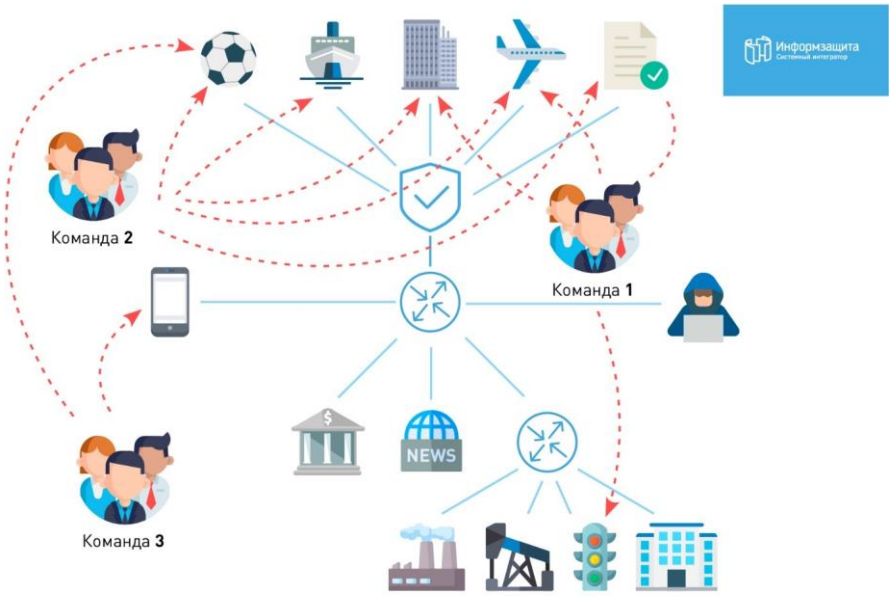
После совместного выступления с ЦАРК-ой на сцене меняем парадигму с «нужно набрать ещё баллов», на «нужно не дать ЦАРК-е набрать ещё баллов».

На одном из наших серверов запускаем Cain&Abel и переводим весь трафик на наш сервер. Находим несколько казахских VPN-ов, «рубим» их.

В итоге решаем зарубить весь трафик, настраиваем локальный фаервол на шлюзе на запрет всего трафика в АСУ ТП сеть (вот как надо защищать АСУ ТП). Прибегают организаторы и говорят, что у них не работает доступ к АСУ ТП. Пропиливаем им доступы для их IP-адресов (вот как не надо защищать АСУ ТП).

12:47
Не зря нервничали. Организаторы подкидывают очередной сюрприз. Откуда ни возьмись всплывает по четыре доменных учётки к каждому домену. Мобилизируем команду.

Задача Команды-1 — как можно глубже и быстрее залезть в защищенные сегменты. Задача Команды-2 — используя Outlook Web Access сменить пароли учетным записям. Некоторые защитники, что-то западозрив, просто отключают VPN. Некоторые поступают хитрее — переводят свои системы на китайский язык. Функционал работает, но при этом пользоваться невозможно (орги, ау!). Через VPN подключаемся к трем сетям. Из первой нас выкидывает через минуту.



12:52
Находим в сети behealthy сервер, уязвимый к MS17-010 (защищённый! сегмент). Эксплуатируем, не встречая сопротивления, получаем хэш администратора домена и через Pth заходим на домен-контроллер. Угадайте, что мы там находим? Обратимое шифрование!

Похоже те, кто защищал этот сегмент, плохо сделали домашнее задание. Получаем всю информацию для тасков, кроме части, связанной с 1С. Есть вариант поковырять её ещё 40-50 минут, но мы решаем просто уронить домен. Конкуренты нам не нужны.

13:20
Сдаем задания: у нас 2.900.000 баллов и несколько непринятых баг баунти. У ЦАРКи чуть больше 1 млн. Они сдают свою криптовалюту и поднимают 200 т. Мы уже не сильно боимся, догнать нас практически нереально.

13:55
Подходят люди, поздравляют. Мы всё ещё боимся какой-то подставы, но похоже нет, мы реально чемпионы!

Вот такая хроника 28 часов от True0xA3. Много что осталось за кадром. Например, выходы на сцену, мучения Wi-Fi и GSM, общение с репортёрами, но мне кажется это не самое интересное.

Это был очень крутой опыт для нас всех и надеюсь, что мне удалось передать хотя бы немного ту атмосферу, которая окружала нас всё это время и показать, насколько интересно участвовать самим. Впереди ещё одна, последняя статья, в которой мы оценим наши ошибки, и постараемся составить план их исправления. Ведь нет ничего лучше, чем учиться на чужих ошибках.

Подробнее: https://habr.com/ru/post/454366/

Компания «Информзащита»
Тел.: +7 (495) 980-2345
E-mail: pr@infosec.ru