Хроники взлома города F

Издание: Banki.ru, 29 мая 2019 г.

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

Однажды на маленький, но очень гордый город F напали хакеры: захватили СМИ, устроили аварию на нефтезаводе, подключились к светофорам. Но добрые защитники отразили злобные атаки и всех спасли… Нет, это не сюжет нового блокбастера, а практическая игра The Standoff («Противостояние»), прошедшая в рамках девятого международного форума по кибербезопасности Positive Hack Days. Что происходило в городе, на чьей стороне оказалась сила, и, главное, зачем все это вообще нужно?

Итак, город F. Он похож на обычный город, только в миниатюре. Тут есть железная дорога, сотовый оператор, ТЭЦ, банки, офисы различных компаний и даже «умные дома». И пусть здания здесь условные, игрушечные, но вот IT-инфраструктура вполне реальная, используемая «в обычной жизни». Все контроллеры в городе настоящие и дорого стоят. Именно за доступ к этой инфраструктуре идет борьба в игре «Противостояние».

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

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

Добро пожаловать на темную сторону силы!

Хакеры в зависимости от того, чем конкретно они занимаются, могут быть «черными» или «белыми». И выбирать ту или иную сторону силы в зависимости от текущих задач и потребностей. Ведь для того, чтобы что-то защитить, надо сначала это что-то «поломать»: найти уязвимости, определить опасности. А потом уже на основании полученных данных и опыта строить защиту. А дальше идет соревнование между защитниками и нападающими.

Такое же противостояние развернулось вокруг города F: на «темной» стороне — 18 команд атакующих, на «светлой» — шесть команд «защитников», каждая из которых отвечает за свой виртуальный офис. Защитники работают совместно с SOC (Security OperationsCenter) — это центры оперативного мониторинга и реагирования на кибератаки, они помогают расследовать инциденты и проводят мониторинг объектов. В некоторых случаях SOC может брать одну или две команды себе под крыло.

Макет города нужен для визуализации действий атакующих: игрушечные поезда сходят с рельсов, миниатюрные химзаводы взрываются. В реальной жизни подобная атака приведет к таким же последствиям, только заводы и поезда будут настоящими, чтобы этого не случилось, безопасники и тренируются на подобных макетах. Игра нужна обеим сторонам, чтобы «других посмотреть и себя показать».

Он сказал: «Поехали!» и махнул... «мышой»

Схватка началась 21 мая в 10:00 мск. Уже через полчаса одна из атакующих команд — True0xA3 — воспользовавшись простейшей уязвимостью проникла в офис промышленной компании и получила функции администрирования домена. А вскоре после этого они смогли выкрасть финансовый отчет прямо с компьютера главбуха медиахолдинга!

В остальном первый день соревнования прошел достаточно спокойно: нападающим понабилось целых 17 часов, чтобы нащупать слабые места в защите и начать серьезную атаку.

Но и это время хакеры использовали с пользой. Узнав, что в городе есть криптовалюта, нападающие начали «майнить» на всех доступных машинах. «Взяла банк» уже упомянутая команда True0xA3.

Как часто случается, самое интересное началось ночью.

Город засыпает, хакеры активизируются

«Под покровом ночи, в 3:30, одна из команд «разломала» нефтебазу № 1, нарушив функции загрузки. Потом пришел черед второй нефтебазы, взломав которую хакеры вызвали перелив нефти», — делится итогами руководитель отдела безопасности промышленных систем управления Positive Technologies Владимир Назаров. Именно он следит за событиями, развернувшимися в городе. Действительно, утром на нефтяных бочках города F можно было увидеть черные подтеки — следы ночной аварии.

Кроме этого, развернулась нешуточная борьба между двумя командами нападающих — True0xA3 и ЦАРКА — за доступ к промышленной базе. Померившись силами, команды решили действовать сообща, что и привело к заметному учащению удачных хакерских атак.

«Мы захватили контроль над системой управления освещением улиц. Все фонари погасли, чему мы были несказанно рады», — делится успехами капитан команды True0xA3 Виталий Малкин, руководитель отдела анализа защищенности компании «Информзащита». Также, по словам Малкина, совместно с другими атакующими его команда приложила руку к разливу нефти на заводе и остановке процесса ее транспортировки.

Утро добрым не бывает…

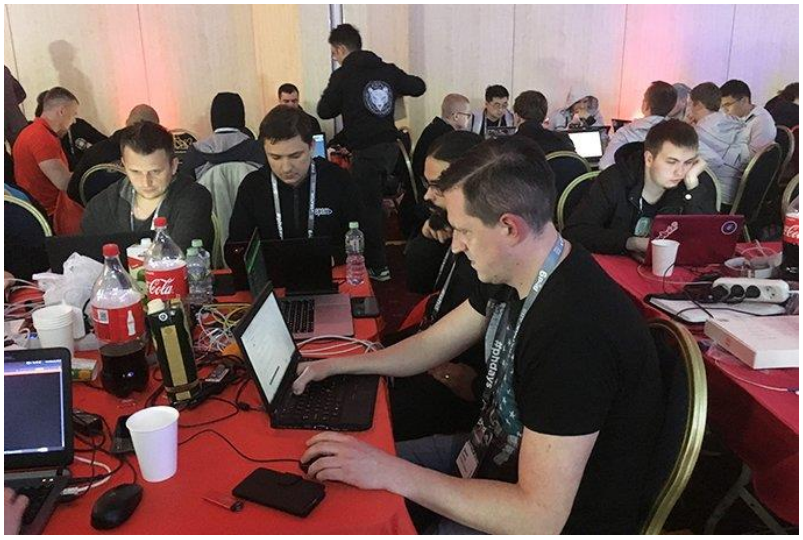
На следующий день, когда участники форума стали собираться на площадке, уставшими выглядели и нападающие, и защитники. Больше суток без сна в напряженной работе — это очень непросто. Кое-где даже можно было увидеть людей, которые выкроили минутку для сна, не покидая рабочего места. Уставшие хакеры и безопасники использовали для отдыха разложенные на площадке пуфики.

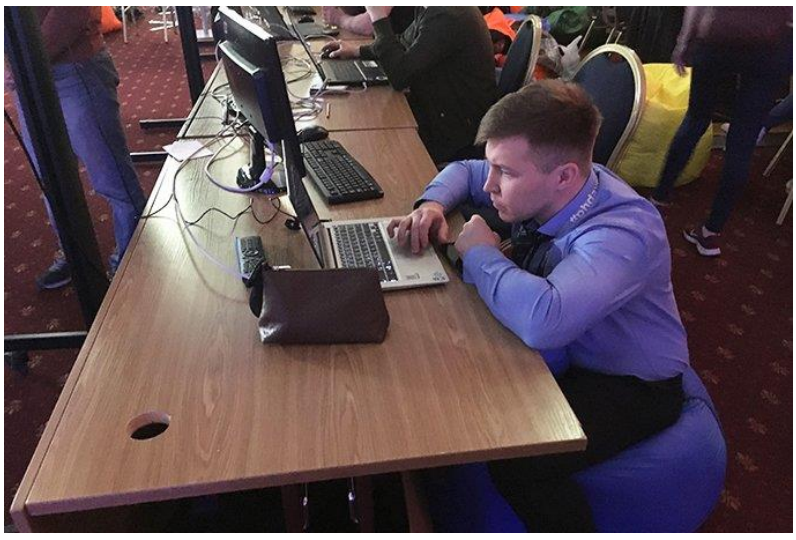
Несмотря на усталость, борьба оставалась напряженной. Произошла полная компроментация офиса страховой компании города F. Это заметила команда защитников под названием STS. Тем временем хакеры нашли в публичных источниках конфиденциальную информацию — доменные учетные записи. К сожалению, не все команды защитников быстро среагировали на новую угрозу. Этим и воспользовалась команда True0xA3, проникнув во внутреннюю сеть с помощью корпоративного VPN. Они получили права администратора за рекордные семь минут, чем и обеспечили себе победу в игре. При этом защитники из STS успели придумать тактику реагирования на произошедшее, но до реализации дело не дошло, игра закончилась в 14:00. За это время, несмотря на усилия защитников, в городе пострадали несколько объектов инфраструктуры, была украдена конфиденциальная информация.

Особенностью этой игры стало то, что борьба шла не только между хакерами и защитниками. Нападающие активно взаимодействовали друг с другом, то сражаясь, то организовывая коалиции. Такие ситуации, кстати, часто случаются и в реальной жизни. А выигрывает сильнейший.

Победители получили денежный приз от организатора, а также путевку на международное киберсоревнование HITB + CyberWeek в Абу-Даби. А вот бесценный опыт приобрели абсолютно все участники соревнований.

Пресса о нас





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

Зачем нужны соревнования?

Эта игра — фактически тренировка для участников рынка кибербезопасности. Многие из тех, кто принимал участие в «Противостоянии», в жизни занимаются примерно тем же. «То, что происходит здесь, по сути для меня и для моей команды — это аналогия того, что мы делаем в реальной жизни, с единственной оговоркой: «Противостояние» в течение двух дней по плотности атак аналогично реальной жизни, но за несколько месяцев. Все происходит так же, но более концентрированно», — поделился капитан команды защитников сотового оператора города F Андрей Дугин, начальник отдела обеспечения информационной безопасности МТС. Кстати, его команда выступила удачно, сотовый оператор города F устоял перед атаками.

Хорошо, если проблемы, организованные хакерами, происходят только в игрушечном мире. И вот уже атакующие «меняют цвет» и возвращаются на рабочие места — обеспечивать защиту реальных компаний и реальных городов. И пусть у них это получается, как можно лучше!

Антонина САМСОНОВА, Banki.ru

Подробнее: https://www.banki.ru/news/daytheme/?id=10897211