Серверная Корея: Как КНДР создала самые эффективные кибервойска в мире

Авторы:

к.т.н., гендиректор ООО ТСС

Александр Атаманов;

к.т.н., гендиректор «Лаборатории Цифровой Форензики» Александр Мамаев.

Подготовлено для Российского совета по международным делам

РСМД

Российский совет по международным делам

Оглавление

Введение

В 2016 г., когда орфографическая ошибка помешала хакерам из КНДР похитить 1 млрд долл. из Федерального резервного банка Нью-Йорка, интернет-пользователи подняли программистов на смех. Однако экспертам, занимающимся расследованиями киберпреступлений, не до смеха: на сегодняшний день Пхеньян имеет в своем распоряжении одну из самых боеспособных и опасных в мире армий хакеров, по численности сопоставимую с кибервойсками США.

В последние месяцы на фоне исторических встреч лидеров Северной и Южной Кореи, а также саммита Ким Чен Ын — Дональд Трамп активизировались разговоры о скором «ядерном перемирии» между Пхеньяном и остальным миром. Переговорной позиции КНДР в этом вопросе помогают и успехи в цифровом секторе: на сегодняшний день Пхеньян обладает эффективным кибероружием, ущерб от которого может оказаться настолько же серьезным, как и от атомной бомбы.

Александр Атаманов — к.т.н., основатель компании ТСС (производит средства криптографической защиты информации) и Александр Мамаев — к.т.н., гендиректор «Лаборатории Цифровой Форензики» (специализируется на расследованиях киберинцидентов) подготовили масштабное исследование, посвященное становлению кибервойск КНДР, тактике и стратегии северокорейских хакеров.

Главные тезисы:

1. КНДР активно развивает кибервойска с 2000-х гг., к настоящему моменту численность группировки сопоставима с силами США (6–7 тыс. человек). Киберсилы КНДР признаются экспертами из США и ЕС одной из самых эффективных и боеспособных киберармий в мире наравне с США, КНР, Россией и Израилем.
2. Тактика кибервойск КНДР прошла через три главных этапа в своем развитии: от «идеологических» атак (на британский *Channel 4* и *Sony Pictures* в 2014 г.) к хакерскому заработку (хищения средств у банков и пользователей, криптомошенничество) и легальному бизнесу в сфере разработок и продаж ПО. По оценкам экспертов, кибератаки приносит КНДР до 1 млрд долл. в год (для сравнения: ВВП КНДР в 2016 г. оценивали в 28 млрд долл.). Четвертым этапом могут стать разрушительные атаки на критическую инфраструктуру Южной Кореи, США и других стран.
3. Кибервойска КНДР уместно разделить на четыре группы, отличающиеся по целям и методам атак:

— *Stardust Chollima* специализируется на «коммерческих атаках»;
— *Silent Chollima* действует против СМИ и государственных учреждений, в первую очередь — южнокорейских;
— *Labyrinth Chollima* фокусируется на противодействии спецслужбам;
— *Ricochet Chollima* занимается хищением данных пользователей.

4. Сама Северная Корея в сравнении с другими странами больше защищена от кибератак, потому что ее инфраструктура слабо интегрирована в Интернет. Отслеживать хакерские атаки КНДР становится все сложнее: уровень подготовки растет, а сами группы рассеяны по всему миру от Японии до стран Ближнего Востока. «Традиционные» методы идентификации организаторов атак (по IP, серверам или «лингвистическим следам» в коде) практически не работают.

Проба кода: к истории вопроса

Ким Чен Ир, руководитель КНДР с 1994 по 2011 г., первоначально расценивал Интернет как потенциальную угрозу режиму. Отношение диктатора стало меняться в середине 1990-х гг., когда в страну по окончании обучения вернулась группа специалистов по компьютерным технологиям. Окончательный разворот произошел после вторжения США в Ирак в 2003 г.: по воспоминаниям известного перебежчика Ким Хун-кванга, Ким Чен Ир заявил: «В XXI в. войны будут вестись в информационном формате».

Пхеньян стал активно прибегать к цифровым технологиям для шпионажа и кибератак. Вскоре хакеры добились первых успехов: в 2009 г. они атаковали сайты в США и Южной Корее, заразив их вирусом *MyDoom*. За нападением стояла группа *Lazarus* (она же *Hidden Cobra*) — самая известная ныне хакерская группировка КНДР.

Однако масштаб КНДР на сетевой карте мира не впечатлял: в 2011 г. на всю страну было зарегистрировано около 1 тыс. IP-адресов — меньше, чем в большинстве кварталов Нью-Йорка.

Все изменилось при Ким Чен Ыне. Впервые мировые СМИ активно заговорили о северокорейских хакерах в 2014 г., и для этого было два повода. В августе киберпреступники атаковали британский телеканал *Channel 4* после того, как тот сообщил, что снимет фильм о британском ученом, похищенном Пхеньяном для разработки ядерного оружия. Серьезного урона атака не нанесла, но это была лишь разминка.

В декабре 2014г. на экраны должен был выйти комедийный боевик Эвана Голдберга и Сета Рогена «Интервью» — фильм, повествующий о двух американских журналистах, отправляющихся в КНДР, чтобы сделать интервью с Ким Чен Ыном и убивающих диктатора по просьбе ЦРУ. Из-за угроз хакеров фильм сняли с проката, а следом *Sony Pictures* подверглась масштабной атаке: киберпреступники проникли на сервера компании, слили в Сеть несколько фильмов, конфиденциальную информацию, а вирус уничтожил до 70% ноутбуков и компьютеров сотрудников компании. На фоне скандала глава студии Эми Паскаль ушла в отставку, а против *Sony* подали многочисленные судебные иски.

Однако постепенно от идеологических атак хакеры перешли к поиску заработка в Сети.

Заработок в Сети

В 2017 г. КНДР заработала около 200 млн долл. на незаконном экспорте угля и оружия, говорится в секретном докладе независимых

наблюдателей ООН. Сделки осуществлялись через порты России, КНР, Малайзии, Вьетнама, Сирии и Мьянмы.

Однако этим список преступных доходов не ограничивается: за последние 20 лет Пхеньян не раз обвиняли в торговле контрафактом (от одежды до сигарет), обороте поддельной валюты, наркоторговле.

Теперь корейские чиновники открыли для себя новый, куда более безопасный способ приработка: хакерские атаки. По словам консультанта Национальной разведывательной службы Южной Кореи Саймона Чой, за последние несколько лет северокорейские хакеры атаковали более 100 банков и криптобирж, похитив более 650 млн долл. Бывший британский разведчик полагает, что киберпреступления приносят КНДР до 1 млрд долл. в год. Для сравнения: экспорт КНДР составляет чуть более 3 млрд долл., а ВВП Северной Кореи в 2016 г. оценивался в 28,6 млрд долл. «Я не удивлюсь, если теперь хакерство играет важную роль в структуре доходов КНДР», — заметил ведущий специалист по Северной Корее, профессор, сотрудник университета Кунмин (Сеул) Андрей Ланьков.

Хакерство — идеальный инструмент для пополнения бюджета КНДР по нескольким причинам:

1. Низкая стоимость входа в бизнес: помимо компьютера, доступа к Интернету и сервера опытному специалисту больше ничего не потребуется;
2. Анонимность пользователя, анонимность денежных транзакций;
3. Вариативность заработка: от выполнения легальных задач на фрилансе до противозаконных таргетированных атак;
4. Возможность уклонения от санкций ООН, в том числе запрета на найм рабочих из КНДР.

Рассмотрим «коммерческие атаки» КНДР подробнее.

Дело на миллиард: Центробанк Бангладеш

В 2015 г. группировки, связанные с Пхеньяном, атаковали онлайн-банки на Филиппинах, во Вьетнаме (*Tien Phong*), в феврале 2016 г. — в Бангладеш. Именно атака на Центральный банк Бангладеш стала одной из самых успешных и самых показательных. Хакерам удалось получить доступ к учетным записям сотрудников банка и взломать систему *SWIFT* (Общество всемирных межбанковских финансовых телекоммуникаций), которой пользуются 11 тыс. банков и других финорганизаций по всему миру. Взлом *SWIFT* потребовался для того, чтобы впоследствии стереть информацию о незаконных переводах.

Преступники направили от лица Центробанка Бангладеш запрос на перевод почти 1 млрд долл. из Федерального резервного банка Нью-Йорка, где хранились средства азиатского государства. Запрос поступил в четверг вечером, когда сотрудники ЦБ уже покинули офис (в пятницу в

Бангладеш выходной). Хакеров подвела всего одна орфографическая ошибка: в документах значилось «*fandation*» вместо «*foundation*». Большая часть перевода была заблокирована, но хакерам удалось вывести 81 млн долл. и обналичить их через филиппинские казино. Это один из первых случаев, когда кибератака использовалась государством не для шпионажа или политических целей, а с прицелом на прибыль.

Технический комментарий: хакеры использовали при атаке вредоносный код evtdiag.exe, внесший незначительные изменения в код ПО Access Alliance. Мошенники модифицировали базу данных, в которую сеть SWIFT записывала информацию об осуществляемых денежных переводах. Вредоносное ПО стирало исходящие запросы на трансфер средств и перехватывало входящие сообщения, подтверждающие транзакцию. Кроме того, под контролем находились хранящиеся на счету суммы с целью предотвращения обнаружения атаки, пока все средства не будут переведены на нужные счета. Наконец, ПО манипулировало принтерами, печатающими физические копии запросов на трансфер денег.

Атака стала возможной в силу отсутствия в системе защиты ЦБ Бангладеш межсетевого экрана (МЭ) и использования дешевых коммутаторов, подключенных к SWIFT. Другая причина, обеспечившая успех взлома, — упущения в защите: помещение, где находились четыре сервера и четыре монитора, располагалась в небольшой пристройке банка.

Проникновение привело к изменению требований по информационной безопасности для всех участников системы SWIFT, которые вступили в силу с января 2017 г.

Поторопились: преждевременный удар WannaCry

В мае 2017 г. Интернет парализовал сетевой червь *WannaCry*, шифрующий все хранящиеся на компьютере файлы и требующий выкуп за разблокировку. За первые четыре дня атаки от червя пострадали около 300 тыс. пользователей в 150 странах мира, ущерб от атаки оценивается в 1 млрд долл.

Специалисты «Лаборатории Касперского» и антивирусной компании *Symantec* обратили внимание, что сигнатуры кода *WannaCry* совпадают с сигнатурой кода, использовавшегося в феврале 2015 г. хакерской группой *Lazarus*. Это более чем явное свидетельство причастности КНДР.

Однако вряд ли стоит утверждать, что атака была намеренной: скорее всего, Пхеньян тестировал этот метод атаки. К такой идее подталкивают несколько соображений:

1. От WannaCry пострадали среди прочих Китай и Россия. Жертвами червя в КНР стали 30 тыс. организаций: больницы, университеты, торговые центры, АЗС и железнодорожные станции. КНР и РФ являются главными геополитическими и торговыми партнерами КНДР, поэтому сомнительно, что Пхеньян нанес намеренный удар по союзникам.
2. Незначительный финансовый результат. Заработав всего от 40 до 70 тыс. долл. на атаке, вряд ли хакеры могут считать операцию успешной: адресные атаки приносят куда больше денег.

Не исключено, что это лишь подготовительный этап в разработке мощного кибероружия или тестирование уже созданных наработок.

Тем не менее WannaCry уместно отнести к коммерческим разработкам, нацеленным как на извлечение прибыли, так и на слежку за финансовыми организациями.

Технический комментарий: специалисты ТСС внимательно изучили исходный код вредоносной программы. Выяснилось, что WannaCry — эксплойт, с помощью которого происходит заражение, и одновременно шифровальщик, загружаемый на компьютер после заражения.

WannaCry распространяется через протоколы обмена файлами, установленными на автоматизированные рабочие станции. Проникнув в папку с документами, вирус шифровал их, изменяя расширение на .WNCRY, после чего требовал от пользователя приобрести специальный ключ для разблокировки. В противном случае хакеры угрожали удалить все файлы. Наибольший урон был нанесен компьютерам под управлением 64-разрядной версии ОС Windows 7.

Крадущаяся кобра, затаившийся эксплойт

В феврале 2017 г. *SIEM*-система помогла предотвратить атаку на польский финансовый регулятор — Комиссию по финансовому надзору. Хакеры модифицировали один из файлов *JavaScript* и разместили на ресурсе вредоносный JS-скрипт, подгружавший вредоносное ПО. Оказавшись в системе, вредоносная программа связывалась с размещенными за границей серверами и осуществляла различные действия с целью разведки и хищения данных.

Примечательно, что программа действовала адресно: хакеры подготовили список интернет-адресов 103 организаций (большинство из них — банки, причем как польские, так и зарубежные, включая кредитные организации Бразилии, Чили, Эстонии, Мексики и даже *Bank of America*), чтобы целенаправленно заразить сотрудников указанных структур. В случае успеха хакеры смогли бы получить контроль и над финансовыми потоками, но в первую очередь их интересовала информация о рынке, а не хищение средств.

В марте 2018 г. турецкие СМИ со ссылкой на *McAfee* сообщали об операции хакеров против финансовой системы Турции. В силу сходства кода, бизнес-специализации жертвы и наличия строк сервера управления атака была идентична предыдущим нападениям *Hidden Cobra (Lazarus)*, проведенным против глобальной финансовой сети *SWIFT*. Фишинговые письма включали файлы *Microsoft Word*, содержащие встроенный эксплойт *Adobe Flash*. Однако в процессе расследования аналитики выяснили, что операция в Турции была лишь частью масштабной операции *Ghost Secret*, затронувшей в общей сложности 17 стран и нацеленной на сбор информации о критической инфраструктуре, телекоммуникациях и даже развлекательных организациях.

Предполагается, что уязвимости нулевого дня в *Adobe Flash* были найдены именно северокорейскими хакерами и долгое время замалчивались. Группа встроенных вредоносных файлов *SWF* в программе позволяет получить полный контроль над компьютерами жертвы. После того как *Adobe* выпустила патч для безопасности, хакеры модифицировали вредоносное ПО, чтобы нацелиться на европейские финансовые учреждения, предоставляя им возможность красть конфиденциальную информацию о рынке.

Затишье перед кибербурей: когда замаячит блэкаут

В начале 2018 г. аналитики *FireEye* (входит в топ-10 мирового рейтинга компаний по кибербезопасности, является одним из основоположников систем защиты от угроз «нулевого дня») отчитались о разрушительной деятельности группировки *APT37* (она же *Reaper*), продемонстрировавшей сложные высокоуровневые возможности взлома. Директор аналитического отдела разведки в *FireEye* Джон Хальквист заметил, что эти хакеры «не стесняются: они чрезвычайно агрессивны». В докладе *FireEye* отмечалось, что главной задачей *APT37* является «тайный сбор разведданных для поддержки стратегических военных, политических и экономических интересов КНДР».

В отличие от *Lazarus*, *APT37* намеренно работает в тени и старается не попадать в поле внимания, ее деятельность охватывает регион от Азии до Ближнего Востока, атаки становятся все более изощренными. *FireEye* полагает, что *APT37* была основана в 2012 г. и базируется в Северной Корее. В настоящий момент сфера их интересов простирается от энергетического сектора, нефтепромышленности, электроники до автомобилестроения и аэрокосмической отрасли. Тактика хакеров

варьируется от уничтожения данных пользователей до получения полного скрытого контроля над АРМ. Используя фишинговые методы и распространяя вредоносную программу *DogCall*, злоумышленники делали скриншоты страниц и заполучали пароли пользователей — сотрудников южнокорейского правительства в марте и апреле 2017г. Благодаря этому хакерам удалось похитить военные документы, в том числе совместные оперативно-боевые планы Южной Кореи и США по конфликту с Пхеньяном. Также жертвами хакеров стали ближневосточная телекоммуникационная компания и вьетнамская торговая компания.

В статье *Wall Street Journal* отмечается, что за последние 18 месяцев следы хакеров из КНДР прослеживаются во все большем количестве кибератак, «уровень хакеров серьезно улучшился», а цели становятся более тревожными.

В 2017 г. Министерство торговли, промышленности и энергетики Южной Кореи сообщило, что за 10 лет количество попыток доступа к государственным энергетическим компаниям *Korea Electric Power Corporation (KEPCO)* и *Korea Hydro&Nuclear Power (KHN*P) увеличилось в 4 тыс. раз. По меньшей мере 19 атак на *KEPCO* были осуществлены с территории КНДР.

Это очень тревожный сигнал, свидетельствующий о том, что Пхеньян может получить контроль над энергетическим сектором и уже давно «приценивается» к отрасли. Еще в 2014 г. хакеры получили доступ к информации китайского ядерного оператора KHNP, сотрудничающего с Южной Кореей. Хотя южнокорейские официальные лица утверждали, что критические данные украдены не были, факт совершенной атаки настораживает.

В сентябре 2017 г. фирма из Мериленда *Dragos* (специализируется на уязвимостях промсектора) индексировала подозрительную активность группировки *Covellite*, нацелившейся на энергосистему в США, Европе и странах Восточной Азии. Методы злоумышленников очень напоминали активность *Lazarus*. Хоть в компании и не стали напрямую связывать группу с Пхеньяном, правительство США открыто обозначило хакеров как членов *Lazarus*.

При этом аналитики отметили, что *Covellite* не продемонстрировала «должного профессионализма». Однако не стоит торопиться с выводами: не исключено, что эти действия были попыткой «обозначить намерения» или «прощупывание» слабых мест системы.

В отличие от Южной Кореи, энергосистема США сложнее для взлома: здесь много частных, независимых друг от друга поставщиков. Зачастую на предприятиях используются устаревшие ручные системы управления, что усложняет задачи в сравнении с Южной Кореей.

Эксперты *Dragos* предположили, что злоумышленники могут разрабатывать вредоносные программы, способные привести к полному отключению электросети США. Более половины уязвимостей, выявленных в промсекторе США, потенциально могут привести к «сильному операционному воздействию», говорится в январском отчете *Dragos*. Компания проанализировала 163 новых уязвимости безопасности, появившихся в прошлом году в компонентах промышленного контроля, и обнаружила, что 61% из них, вероятно, вызовут «серьезное оперативное воздействие», если будут использованы в кибератаке. Большинство уязвимостей могут использоваться лишь в том случае, если злоумышленник получил доступ к сети предприятия. Однако озабоченность вызывает то, как оперативно производители оборудования оповещают коммунальные службы о дырах в безопасности. Зачастую они ничего не предпринимают , даже если уязвимости уже обнаружены и описаны. Контроль над энергосистемой может стать мощным козырем в переговорах Пхеньяна с Вашингтоном.

Но этим арсенал КНДР не ограничивается: хакеры продолжают разработки. Министерство внутренней безопасности США сообщило о том, что в декабре 2017 г. обнаружило «разрушительное вредоносное ПО» *SMASHINGCOCONUT*, за которым может стоять КНДР. По словам аналитика службы безопасности *Symantec* Эрика Чиена, если Пхеньян действительно стоит за атакой *SMASHINGCOCONUT*, это отражает сдвиг в стратегии КНДР, в последние годы сосредоточившейся на нападении на финансовые учреждения и криптовалютных операциях.

Технический комментарий: SMASHINGCOCONUT — 32-битное вредоносное ПО на базе Microsoft Windows, способное сделать систему на базе Windows неоперабельной. После установки вредоносного ПО хакер должен вставить аргумент командной строки для выполнения, и вредонос удалит все файлы, а также закодирует все данные на компьютере.

Помимо адресных и рассеянных кибератак, КНДР заинтересовалась возможностью слежки за пользователями и сбором конфиденциальных данных. Так, в *Google Play* в течение двух месяцев (с января по март 2018 г.) были доступны три приложения, собирающие информацию об устройстве, личные фотографии, а также копирующие контакты и текстовые сообщения.

Приложения были нацелены на перебежчиков из Северной Кореи, обосновавшихся в других странах, прежде всего — в Южной Корее. Любопытно, что приложения скачали всего около 100 раз, но в этом и заключалась цель: разработчики программ-шпионов зачастую заражают

небольшое количество тщательно отобранных целей, чтобы оставаться незамеченными администрацией маркетов.

О северокорейском происхождении приложений свидетельствовали несколько фактов: аналитики *McAfee* обнаружили в коде уникальные корейские слова, не используемые жителями Южной Кореи; в файле текстового журнала значился северокорейский IP-адрес. При этом разработчики, по всей видимости, не связаны с идентифицированными ранее хакерами. Новую группу назвали *SunTeam*. Не исключено, что это одно из подразделений *Lazarus*.

Также Пхеньян занимается разработками в слежке за пользователями *iPhone*. В мае 2018 г. исследователь кибербезопасности Дариен Гусс из компании *Proofpoint* обнаружил программу — инструмент управления мобильными устройствами (MDM), позволяющую предприятию удаленно контролировать корпоративные смартфоны *iPhone*, которыми пользуются сотрудники. Приложение размещалось на сервере, где, как предполагается, расположены и другие инструменты взлома за авторством программистов из Северной Кореи. Приложение позволяет полностью следить за пользователями *iPhone*: их перемещением, контактами, сообщениями.

Не исключено, что этим набором инструментов против *iPhone* дело не ограничивается. Тем более что аналогичными разработками занимаются и другие страны. Например, израильской компании *Cellebrite* удалось взломать *iPhone*. Интересно, что компания является подрядчиком американского правительства.

Криптовалютный ажиотаж

Повышенный интерес властей КНДР к криптовалютам заслуживает отдельного внимания. За 9 лет с момента запуска биткоина криптовалюты из увлечения энтузиастов превратились в полноценный финансовый инструмент. В декабре 2017 г., на пике рынка, капитализация рынка криптовалют превысила 500 млрд долл. На данный момент на цифровых биржах обращается более 1100 криптовалют, количество активных пользователей виртуальных кошельков, хранящих криптовалюты, выросло с 2,9 млн в 2013 г. до 5,8 млн человек в 2017 г.

Согласно докладу Кембриджского центра альтернативных финансов (*CCAF*), большинство обладателей криптовалют (более 60%) проживают в Северной Америке и Европе, еще 20% — в Азиатско-Тихоокеанском регионе. Многие страны официально признали криптовалюты финансовым инструментом или платежным средством: Европейский суд в 2015 г. отнес транзакции в биткоинах к платежным операциям с валютами, монетами и банкнотами, рекомендовав членам ЕС не облагать операции НДС; Япония признала биткоин законным платежным средством в марте 2016 г.; Китай классифицировал криптовалюту как товар; Минфин США объявил биткоин «децентрализованной виртуальной валютой», а Швейцария приравняла его к иностранным валютам, которые имеют право на оборот и прием к оплате в стране.

В октябре 2017 г. по итогам совещания с министром финансов Антоном Силуановым, помощником Андреем Белоусовым и председателем ЦБ Эльвирой Набиуллиной президент России Владимир Путин поручил к 1 июля 2018 г. прописать в российском законодательстве статус криптовалют, токенов, смарт-контрактов и технологии блокчейна; установить требования к майнерам, включая регистрацию указанных субъектов, а также определить порядок налогообложения; урегулировать публичное привлечение денежных средств и криптовалют путем размещения токенов (ICO) по аналогии с первичным размещением ценных бумаг (IPO). Пока что на поручении история и остановилась.

Но криптопроекты, как и другие компании, не всегда защищены от киберугроз. В разное время жертвами хакеров становились криптобиржи *MtGox*, *Bitfinex* и NEM, венчурный фонд *The DAO*, торговая площадка *Coincheck*, онлайн-рынок для майнинга криптовалют *NiceHash*.

Криптокошельки оказываются не более надежными: по оценкам *High-Tech Bridge*, более 90% популярных криптокошельков, представленных в *Google Play*, подвержены уязвимостям того или иного рода.

Технический комментарий: эксперты изучили как приложения с числом установок до 100 тыс., так и те, количество инсталляций которых превышает 500 тыс. Как оказалось, 93% программ с числом установок до 100 тыс. содержат по меньшей мере 3 уязвимости среднего уровня опасности, в 90% приложений из данной категории было обнаружено по меньшей мере 2 опасные проблемы. Также выяснилось, что 87% кошельков уязвимы к атакам «человек посередине», позволяющей перехват информации, 66% приложений содержат вшитые конфиденциальные данные (в том числе пароли и ключи API), 57% приложений используют функционал, подвергающий риску конфиденциальность пользователя, 80% приложений отправляют данные в незашифрованном виде по HTTP, 30% применяют ненадежное либо неэффективное шифрование, 77% приложений используют SSLv3 или TLS 1.0, бэкенды (API или web-сервисы) 44% приложений оказались уязвимы к атаке Poodle. 100% приложений не имеют защиты против реверс-инжиниринга.

По оценкам *Group-IB*, общий ущерб от целевых хакерских атак на криптоиндустрию в 2017 г. составил более 160 млн долл., доход от хакерских атак на криптобиржи варьируется от 1,5 до 72 млн долл., в то время как в результате успешной атаки на банк преступники в среднем зарабатывают всего 1,5 млн долл.

Неудивительно, что КНДР активно интересуется криптотемой: аналитики ТСС еще в 2013 г. идентифицировали на форумах, посвященных биткоину, IP-адреса, связанные с Северной Кореей.

Южная Корея — один из локомотивов криптоиндустрии. Именно местные проекты первыми пострадали от северокорейских хакеров. Например, *Youbit* в декабре 2017 г. «потеряла» 17% цифровых денег и вскоре обанкротилась. Тогда курс биткоина достиг 20 тыс. долл., а в апреле мошенникам удалось похитить биткоинов на 36 млн долл. В Сеуле также подозревают Пхеньян в хищении 523 млн долл. у японского обменника *Coincheck*.

Жертвами хакеров становились и частные инвесторы. В 2017 г. хакеры из КНДР начали массово создавать в *Facebook* фиктивные профили привлекательных девушек, якобы интересующихся биткоином и работающих в криптоотрасли. В профилях фигурировали «Исследовательский центр *NYU*» и другие учреждения, не вызывающие подозрений. Хакеры заводили знакомства с мужчинами-пользователями криптобирж, затем отправляли файлы *Microsoft Word*, замаскированные под открытки или приглашения, заражая ПО пользователей и получая доступ к криптосредствам, рассказывали аналитики, знакомые с расследованием.

Еще один способ извлечения прибыли — заражение рабочих станций вирусом для майнинга криптовалют. В январе 2018 г. американская фирма *Alien Vault* обнаружила фрагмент вредоносного ПО, устанавливающего приложение на компьютер жертвы, чтобы добыть валюту *Monero*.

Технический комментарий: в практике «Лаборатории Цифровой Форензики» было зарегистрировано как минимум два случая заражения компьютерных сетей вирусом для майнинга Monero. Анализ кода вредоносной программы позволяет утверждать, что в атаке использовались эксплойты, идентичные предыдущим атакам, приписываемым северокорейским хакерам.

Интерес КНДР к *Monero* не случаен. Биткоин остается самой популярной криптовалютой в мире. Одна из ключевых характеристик валюты, привлекающая криптоэнтузиастов, — «анонимность» транзакций: переводы в биткоинах, предположительно, невозможно отследить. Однако с недавних пор ситуация изменилась: в начале 2018 г. поставщик блокчейн-решений *Bitfury Group* представил набор инструментов *Crystal*, позволяющий сотрудникам правоохранительных органов и частным экспертам отслеживать пути подозрительных транзакций до конечного получателя или точки сбыта криптовалюты. Сервис устанавливает связь между предполагаемыми злоумышленниками, позволяет определять вероятность причастности отдельных адресов к незаконной деятельности. И это не единственное решение, представленное на рынке. *Monero* пока не так популярна, как биткоин, но ее уровень безопасности сегодня оценивается выше.

ПО на экспорт: легальный бизнес

Сделав ставку на развитие кибервойск, КНДР достигла больших успехов в подготовке квалифицированных IT-кадров. В 2015 г. на международном конкурсе *CodeChef*, организуемом индийской IT-компанией, северокорейские команды заняли первое, второе и третье места из более чем 7 600 участников со всего мира. Три из 15 лучших кодеров в сети *CodeChef*, насчитывающей около 100 тыс. пользователей, - представители КНДР.

Неудивительно, что Пхеньян начал активно развивать IT-бизнес — причем так, что связей с КНДР у этих компаний не прослеживается. Согласно докладу Центра исследований проблем нераспространения Джеймса Мартина, компании, связанные с властями КНДР, создают и продают разнообразное программное обеспечение по всему миру: от разработки и администрирования сайтов, программ-шифровальщиков файлов до *VPN*-построителей, систем аутентификации и распознавания лиц.

Одна из «корневых» фирм — оборонная *Global Communications (Glocom)*, создавшая сеть фирм по всей Азии. Аффилированная с *Global Communications* компания *Future Tech Group* не так давно выиграла престижную награду за программу распознавания лиц на конкурсе в Швейцарии. Также *Future Tech Group* продвигала проекты веб-разработки в американских школах, продавала ПО для распознавания лиц правоохранительным органам Турции и других стран.

Еще одна аффилированная с *Glocom* компания — *Adnet International* — предлагает методы идентификации биометрических данных для клиентов в Китае, Японии, Малайзии, Индии, Пакистане, Таиланде, ОАЭ, Великобритании, Германии, Франции, России, Канаде, Аргентине, Нигерии. *VPN*-технологии, разработанные северокорейскими компаниями, продавались в Малайзии.

Фирмам удается скрывать связи с правительством посредством создания цепочек-посредников в разных странах мира. Получается, что формально Пхеньян отношения к бизнесу не имеет. Но заказы открывают перед Пхеньяном как колоссальный простор для деятельности, так и «ящик Пандоры» для заказчиков КНДР.

Во-первых, никто не знает, не скрыты ли в ПО бэкдоры — дефекты алгоритма, намеренно встраиваемые разработчиком и позволяющие получить несанкционированный доступ к данным или управлению операционной системой и компьютером в целом. Не исключено, что разработчики из КНДР намеренно оставляют закладки в программах, чтобы в нужный момент проникнуть в систему и получить полный контроль над ней.

Во-вторых, теоретически Пхеньян может сформировать колоссальную базу данных частных лиц и организаций. Предоставляя программы распознавания лиц и отпечатков пальцев, они создают условия для сбора информации о пользователях. Эти данные впоследствии могут быть использованы для обхода двухфакторной аутентификации в онлайн-банкинге или на других ресурсах, где требуется предоставление биометрических сведений.

«Портрет» северокорейских хакеров

Пусть почти никто в КНДР не имеет широкого доступа к интернету, Пхеньяну удалось взрастить армию высококвалифицированных хакеров, укомплектованную из лучших студентов-математиков, которые становятся негласной элитой страны.

Профессор информатики из КНДР Ким Хеунг Кванг, в 2004 г. бежавший в Южную Корею, утверждал, что на службе Пхеньяна 6 тыс. хакеров, которые отчитываются напрямую перед Генеральным бюро разведки. Для сравнения: американское Киберкомандование, созданное Бараком Обамой в 2009 г., насчитывает около 700 военных и гражданских служащих. Киберподразделения в военных службах США насчитывают 6200 человек. И в Штатах признают опасность угрозы: командующий сил США на Корейском полуострове Винсент Брукс уверен, что северокорейские хакеры — «одни из лучших в мире и самые организованные». Вице-президент *CrowdStrike* Адам Мейерс соглашается, что КНДР — «это грозный киберпротивник».

«Потенциал Северной Кореи по уничтожению критической инфраструктуры без ядерного оружия в значительной степени игнорируется, но у Пхеньяна достаточно кибернетических возможностей для нанесения серьезного ущерба», — отмечали Дунхуэй Парк и Джессика Бейер.

Британский парламентский Комитет по обороне в докладе отметил, что северокорейские кибератаки, по всей видимости, представляют большую угрозу, чем ядерные ракеты. Парламентарии призвали увеличить инвестиции в обеспечение кибербезопасности королевства, но вне рамок оборонного бюджета. При этом англичане посетовали на острую нехватку квалифицированных кадров (с чем Пхеньян не сталкивается).

WSJ разделяет киберподразделения КНДР на три группы, основываясь на заявлениях перебежчиков и южнокорейских исследователей:

- «Группа А» атакует иностранные объекты и связана с наиболее громкими кампаниями КНДР, такими, как атаки *WannaCry* и *Sony;*
- «Группа В» ориентируется на Южную Корею, военные и инфраструктурные секреты;
- «Группа С» выполняет низкоквалифицированную работу — например, целевые атаки по электронной почте.

Однако уместнее оперировать другой классификацией, впервые использованной экспертами*CrowdStrike*(компания имеет клиентов в 170 странах мира, участвовала в расследовании атак на *Sony Pictures* и Демократическую партию США). Их методика учитывает не только

цели, но и методы группировок. Аналитики использовали корневым словом в названии *Chollima* («Чхоллима») — мифического крылатого коня, почитаемого в КНДР.

Группу *Lazarus* не стоит считать единой организацией: ее уместно разделить на четыре подразделения:

- *Stardust Chollima* специализируется на «коммерческих атаках», приносящих доход;
- *Silent Chollima* действует против СМИ и государственных учреждений;
- *Labyrinth Chollima* фокусируется на противодействии спецслужбам;
- *Ricochet Chollima* отвечает за хищение конфиденциальных данных пользователей.

В последнее время в Сети замечена еще одна группировка, по всей видимости, не связанная с *Lazarus*, старающаяся не попадать в поле зрения и не привлекать к себе внимания: *APT37*, причастная к серьезным проникновениям в системы различных государств от Южной Кореи до стран Ближнего Востока.

По словам перебежчиков и южнокорейских экспертов в области киберразведки, перспективных кандидатов начинают отбирать с 11 лет и направляют в специальные школы, где обучают основам кибербезопасности и разработке компьютерных программ. Киберсолдатам положены соответствующие поблажки: они не беспокоятся о содержании, им доступны продукты, незнакомые другим гражданам, они могут перевезти в Пхеньян всю свои семью. Также киберсолдаты освобождаются от обязательной воинской обязанности — у них другая служба.

Однако есть и обратная сторона: элитный статус имеют элитные киберсолдаты. Но, как и в каждой армии, есть «пехота», находящаяся совсем в другом положении. *Bloomberg* пообщался с северокорейцем Чен Хёком, работавшим в кибервойсках КНДР. В репортаже содержится огромное количество данных, но проверить достоверность всех утверждений не представляется возможным.

По словам хакера, он не участвовал в громких операциях и занимался исключительно зарабатыванием денег. Чен Хёк попал на факультет компьютерных войск по распределению, учился в Китае, по возвращении на родину поступил в кибервойска, после чего его отправили в КНР на заработки. На компьютер хакеру пришлось заработать самостоятельно: вначале он пользовался ноутбуком соседей по общежитию. Первые деньги Чен Хёк получил за торговлю программным обеспечением, затем занялся взломом программ по заказу, в свободное время разорял

игорные сайты, развивал персонажей в онлайн-играх с последующей перепродажей.

Тех хакеров, кто не зарабатывал положенную норму в 100 тыс. долл. в год, отправляли обратно в КНДР. Программистам разрешалось удерживать не больше 10% от прибыли.

После инцидента с госслужащим Чен Хёк сбежал в Бангкок, купив поддельный паспорт, и обратился за помощью в посольство Южной Кореи. Хакеру помогли начать новую жизнь в Сеуле.

Помимо взлома, кибервойска занимаются и другими задачами: по заказу хакеры пишут программы *iOS* и *Android*, а прибыль поступает в казну КНДР. «Филиалы» северокорейских подразделений рассеяны по всему миру, но большинство хакеров проживают в КНР. Учитывая объемы трафика и тщательный мониторинг интернет-запросов пользователей, китайские власти наверняка в курсе деятельности северокорейцев, однако никаких известных мер против кибермошенников предпринято не было. По всей видимости, КНДР и КНР придерживаются молчаливой конвенции о сетевом ненападении.

Заключение

Между кибератаками северокорейских хакеров и ядерными испытаниями прослеживается довольно четкая корреляция: зачастую они совпадают по времени. Так, во время третьего тестирования в феврале 2013 г. южнокорейские телевизионные компании и банковский сектор пострадали от атаки 3,20 *CyberTerror*, известной как *Dark Seoul*. В январе 2016 г., когда Северная Корея провела четвертый взрыв, произошла массовая рассылка фишинговых писем южнокорейским должностным лицам. После пятого испытания в сентябре 2016 г. хакерам удалось похитить секретные военные файлы у Южной Кореи. Не исключено, что Пхеньян отвлекает внимание от кибератак ядерными испытаниями: мировым СМИ попросту некогда рассказывать о событиях в ИБ, когда речь идет об атомном взрыве.

Случаи атак на энергосистему Южной Кореи и США свидетельствуют о том, что КНДР могла начать подготовку к четвертому этапу собственной киберстратегии: последующие удары могут быть направлены на критическую инфраструктуру, и предсказать последствия пока что не представляется возможным.

Прозвучит парадоксально, но изоляция КНДР усложняет выработку эффективной стратегии против кибератак Пхеньяна: Вашингтону приходится опираться на открытые источники информации. Кроме того, попытки нанести ответный удар в киберпространстве заведомо обречены на провал просто потому, что страна практически не имеет выхода в Сеть.

Тем не менее США активизировались в кибернаправлении: в последний год они активно закладывают базис для кибератак против КНДР через Южную Корею и Японию, где расположены многочисленные военные объекты американцев. Подготовка включает прокладку оптоволоконных кабелей, настройку удаленных баз данных, прослушивающих устройств, способных подключиться к северокорейской сети.

Но даже если полностью ограничить доступ КНДР к Сети, атаки не прекратятся: северокорейские хакеры рассеяны по всему миру и могут продолжать нападения из любой точки Юго-Восточной Азии, где есть доступ к интернету. При этом наказать Пхеньян за киберпреступления невозможно: наиболее болезненные санкции против страны уже введены, а на военный удар за кибератаки ни одно государство не решится.

Информация об авторах

Александр Атаманов — к.т.н., основатель и генеральный директор ООО ТСС, отечественного производителя средств информационной безопасности. Вместе с командой разработчиков создал уникальную технологию высокоскоростного шифрования по алгоритму ГОСТ, не имеющую аналогов на отечественном рынке. Выпускник Московского инженерно-физического института по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

Александр Мамаев — к.т.н., сооснователь и генеральный директор судебно-экспертной организации «Лаборатория Цифровой Форензики». 3 года руководил кафедрой «Криптология и дискретная математика» НИЯУ МИФИ. Руководитель проекта сотрудничества НИЯУ МИФИ и Университета Суррей (Великобритания). Участник бизнес-акселератора GVA LaunchGurus - StartupAcademy 5. Проходил стартап-обучение в Кремниевой долине.