Львов В.Е.

Дальневосточный юридический институт МВД России имени И.Ф. Шилова
(г. Хабаровск)

Обеспечение безопасности телекоммуникационных систем

Начнем мы с мотивации, важно понимать, чем именно мотивированы все эти хакеры (атакующие), которые совершают киберпреступления. Классически так сложилось, что выделяются три основные группы.

1 группа – финансово мотивированные, основной целью всегда являлись деньги, финансовая выгода, плюс для этих групп приоритетом является возможность тратить как можно меньше средств в процессе подготовки.

2 группа – проправительственные группировки и хакеры. С меньшим количеством атакующих, но в целом достаточно объемная, при этом обладает более интересными и продвинутыми инструментами (например, Метастилер), в том числе созданными собственноручно, приобретенными в Даркнете, и являются зачастую источниками развития трендов и схем атак.

3 группа – кибертеррористы и хактивисты, например достаточно известная группа «Анонимус». В основе присутствует какая-то идея (правое дело), за которую борются, или проблема, к которой привлекают внимание путем нанесения вреда компаниям или людям, которые против этой идеи. Например, борцы за экологию иногда делают дипфейки. Используются не такие продвинутые инструменты, такие хакеры больше энтузиасты.

Когда кибератаки классифицировать не представляется возможным, выделяется четвертая группа – хакеры с неявной мотивацией. Рамками все далеко не ограничено, есть еще множество вариантов мотиваций: саботаж, шпионаж, попытка доказать самому себе или кому-то свою силу и другие. Появление групп двойного назначения Comet (Shadow) и Twelve.

Кибератака – это развитие инцидента до Cyber Kill chain от начала до конца (разведка → вооружение → доставка → эксплуатация → инсталляция → управление и контроль → действия на объектах).

TTP (тактики, техники и процедуры) – обобщенное описание поведения или действий злоумышленника. Алгоритм разбора инцидента с помощью MITRE ATT&CK (разведка → разработка ресурсов → начальный доступ → исполнение → настойчивость (закрепление) → повышение привилегий → уклонение от обороны (обнаружения) → доступ с учетными данными → открытие (разведка внутренних ресурсов) → боковое перемещение → коллекция (сбор данных) → командование и контроль → эксфильтрация → воздействие деструктивное → мобильный → микросхемы) можно использовать в качестве источника данных о киберугрозах (TI), матрица обновляется исследователями со всего мира.

APT (целевая продолжительная атака) – противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые

позволяют ему создавать угрозу опасных кибератак. Целями APT являются: госучреждения, КИИ, оборонный комплекс, военные учреждения. Зафиксированы случаи компрометации инфраструктуры российских компаний с участием бывших сотрудников (зачастую покинувших пределы страны).

Популярные векторы атаки – компрометация служб удаленного доступа, фишинговые рассылки, а также уязвимости в инфраструктуре компаний-подрядчиков (supply chain).

Кибершпионажем занимаются и прогосударственные группировки стран – не участников конфликта (на примере Северной Кореи, Китая).

Шифровальщики не сдают позиций, используются как ранее слитые программы-шифровальщики, так и легитимные инструменты, например Bitlocker. Основные жертвы – ретейлеры, производственные, строительные, туристические и страховые компании.

Одной из новых тактик, применяемых злоумышленниками, стала кража сессий Telegram-клиентов, установленных на рабочих станциях жертвы.

Группа Comet (Shadow) выступает в роли вымогателя – требует выкуп за расшифровку и нераспространение похищенных данных, они же еще и самые жадные, рекорд – 321 миллион рублей, а Twelve – хактивиста (диверсанта), уничтожающего информационно-телекоммуникационную инфраструктуру жертвы без выставления финансовых требований.

Более 300 облачных хранилищ с логами как источник данных для атак, через которые проходят огромные потоки украденных данных – в основном результаты работы программ-стилеров. Пятикратный рост уникальных скомпрометированных хостов посредством стилеров в крупных банках РФ и СНГ и растет во всем мире.

Agent Tesla – это популярный троян, появившийся в продаже с 2014 г. Сначала создавался как keylogger, но с течением времени получил расширенные функциональные возможности.

Атаки со стороны шифровальщиков остаются одной из важных киберугроз для коммерческих и государственных компаний по всему миру.

Системы искусственного интеллекта не только используются для усовершенствования кибератак злоумышленниками, но также интегрируются в рабочие процессы организаций, что создает новые потенциальные уязвимости.

Наблюдается значительный рост и увеличение сложности атак, а также рост числа атак на поставщиков и посредников, чтобы получить доступ к инфраструктуре жертвы (пример атаки на уязвимость в выполнении SQL запросов в программном обеспечении MOVEit Transfer). Сдвиг фокуса кибератак с Windows и Android на устройства Apple. Рост услуг Fishing-as-a-Service (на андеграудных площадках и в Telegram).

Несмотря на аресты участников преступных групп и захват инфраструктуры вымогателей со стороны правоохранительных органов, криминальный бизнес шифровальщиков продолжает процветать.

Одна из известных атак – операция «Триангуляция». Цель: шпионаж. Используемые инструменты: TriangleDB, JavaScript Validator. Основные техники: Exploit Public-Facing Application, Exploitation for Privilege Escalation, Credentials from Password Store: Keychain, Location Tracking, Ingress Tool Transfer.

Вредоносное программное обеспечение, например трояна удаленного доступа Darktrack RAT и условно легитимного ПО.

Вредоносное программное обеспечение в iMessage → JavaScrip валидатор → эксплойт для WebKit → эксплойт для ядра iOS → бинарный валидатор → имплант TriangleDB → действия на объектах.

Webkit – движок для развертывания веб-страниц (Apple). Он развертывается в памяти, а это означает, что все следы импланта теряются при перезагрузке устройства.

Их методы взлома включают отправку фишинговых писем со ссылками на вредоносные файлы, что позволяет хакерам получать доступ к системам государственных учреждений в России и Беларуси.

В кампании 2023 г. фишинговые письма маскировались под повестки от военного комиссариата Министерства обороны России. В июне-июле была зафиксирована рассылка писем под видом зашифрованного архива с итогами фейкового тендера военного ведомства.

В ноябре 2023 г., атакующие рассылали вредоносный архив от имени курьерской службы доставки Pony Express. Получателями стали как минимум три десятка компаний, в том числе российские банки, ретейлеры и маркетплейсы, телеком-операторы, предприятия агропромышленного комплекса и ТЭК, логистические и ИТ-компании.

Группировка киберпреступников организовывала структуру с отделами (группами), корпоративной иерархией, регулярными зарплатами, системой мотивации и отпусками. Среди задач были мониторинг обновлений Windows и исследование изменений в новых патчах.

Отделы выдавали задания, помогали с актуальными вредоносными файлами и обновлениями, отвечали за работу в сетях и другие технические вопросы, проводили чат-сессии с подчиненными для обсуждения текущих проблем т.е. обеспечивали все условия для того, чтобы команда успешно выполняла свои задачи. В каждой из групп были разработчики, специалисты по OSINT, системный администратор, тестировщик и реверс-инженер. Также среди сотрудников были специалисты по пентесту с опытом в поиске уязвимостей нулевого дня и человек, отвечавший за наполнение DLS-контентом. Он же контролировал отправку ключей жертвам при оплате выкупа. Кроме того, в штате был и специалист по обучению. В группе были хорошо выстроены процессы отбора резюме, переговоров с кандидатами и собеседований.

Перспектива киберпреступлений: рост активности киберпреступников, включая хактивистов и прогосударственных группировок; главной мишенью останутся объекты критической инфраструктуры и организации в госсекторе.

Промышленные предприятия, ядерные станции и научные центры, предприятия водоснабжения, правительственные сайты и системы; рост фишинговых атак через соцсети: Telegram и WhatsApp; набирают популярность фишинговые атаки с использованием искусственного интеллекта для подмены лица и голоса; рост интернет-мошенничества.

Базовый уровень защиты: регулярное обновление ПО; регулярный мониторинг утечек; строгая парольная политика; настройка многофакторной аутентификации учетных записей; аудит и отключение невостребованных удаленных сервисов; запрет регистрации аккаунтов на сторонних сервисах с корпоративной почты.

Продвинутый уровень защиты: блокировка входящих соединений на SMB-порты от хостов вне корпоративной сети; запрет входа на конечные устройства под рутом по SSH; использование минимальных привилегий для учетных записей служб; ограничение сетевого доступа по задачам конкретной учетной записи; аудит нелегитимных сессий Telegram; отслеживание DNS-трафика.

Защита для корпораций: внедрение средств СЗИ; фильтрация входящего трафика; настройка блокировки учетных записей при неверном входе; осуществление непрерывной идентификации теневых информационных технологий для управления поверхностью атаки; регулярная проверка инфраструктуры на уязвимости.

Минаев В.А.,

доктор технических наук, профессор
Московский университет МВД России имени В.Я. Кикотя

Корнилович Р.А.,

кандидат технических наук, доцент
Московский университет МВД России имени В.Я. Кикотя

Фаддеев А.О.,

доктор технических наук, доцент
Московский университет МВД России имени В.Я. Кикотя

Геодинамическая безопасность топливно-энергетического комплекса России

Топливно-энергетический комплекс (ТЭК) России, включающий отрасли, занимающиеся добычей, переработкой и транспортировкой углеводородов, производством, транспортировкой и распределением электроэнергии, является одной из самых важных, но и самых уязвимых, в смысле рисковых ситуаций, частей экономики страны. Структура ТЭК связана не только с