Ростелеком
Солар

Профили киберпреступников

ПРАКТИЧЕСКИЙ ПОДХОД
К ПОСТРОЕНИЮ ЗАЩИТЫ ОТ КИБЕРУГРОЗ

Эволюция ландшафта угроз

Киберзлоумышленники активно эксплуатируют доступные возможности, совершенствуют инструменты и усиливают активность. Несколько факторов можно выделить как наиболее значимые в эволюции ландшафта угроз.

1 АВТОМАТИЗАЦИЯ

В арсенале злоумышленников все больше автоматизированных инструментов: от классических сканеров уязвимостей периметра до поисковых систем для Интернета вещей Shodan и Censys.

1 день в среднем проходит между выявлением критической уязвимости и ее появлением в публичном доступе*.

2 ХАКЕРСКИЕ ИНСТРУМЕНТЫ ПО ПОДПИСКЕ

Сейчас любой желающий без навыков программирования может заказать атаку с использованием шифровальщика. Достаточно оплатить подписку на сервис. Для пользователей даже доступна опция клиентской поддержки.

50 $ - средняя стоимость подписки на сервис Ransomware-as-a-Service для злоумышленника**.

3 ЭВОЛЮЦИЯ ЦЕЛЕЙ АТАК

Нацеленность на кражу денег и монетизацию сейчас присуща только некоторым типам преступников. При этом выросло число атак, нацеленных на захват и контроль инфраструктуры и на проникновение в сеть подрядчика.

200 дней в среднем киберпреступники могут оставаться незамеченными в инфраструктуре организации***.

4 УСЛОЖНЕНИЕ ИНСТРУМЕНТОВ АТАК

Продвинутые киберпреступники совершенствуют свои алгоритмы. Использование легитимных утилит, встраивание вредоносного ПО в системные элементы снижает эффективность базовых средств мониторинга.

Каждую неделю в мире появляется **5 инструментов** для реализации атаки, которые раньше не были известны аналитикам*.

Проявленные тенденции и практические знания, накопленные аналитиками Solar JSOC за 8 лет непрерывного мониторинга, позволяют классифицировать киберзлоумышленников в зависимости от их целей и методов атак. В настоящее время явно выделяются 5 основных типов.

*«Ростелеком-Солар», 2020

** Vade Secure, 2020

***IBM, 2020

Уровень 1. Автоматические сканеры

Ищут ИТ-инфраструктуры с низким уровнем защиты для дальнейшей перепродажи информации о них или использования в массовых атаках.

ИНСТРУМЕНТЫ

Автоматическое сканирование на известные уязвимости периметра (ShellShock, EternalBlue и т. п.).

КАК СЕБЯ ПРОЯВЛЯЮТ

Непрерывно сканируют доступные извне сервисы с различных адресов, в том числе с использованием публичных легитимных инструментов сбора информации: Shodan, Censys и др.

ПРИМЕР ЖЕРТВЫ

Региональная сеть медицинских клиник

Более 50% организаций госсектора на момент подключения к сервисам Solar JSOC содержали уязвимости, взломать которые можно с помощью одних только автоматизированных сканеров.

*«Ростелеком-Солар», 2020

КАК ОБНАРУЖИТЬ АТАКУ

Аномальное поведение часто обнаруживают администраторы системы. Также срабатывает система обнаружения вторжений и модули сигнатурного анализа.

КАК ОТ НИХ ЗАЩИТИТЬСЯ

- WAF
- UTM
- Patch-менеджмент

Уровень 2. Киберхулиганы

Сфокусированы на поиске стандартных уязвимостей с целью прокачки своих навыков и мелкого хулиганства, редко самостоятельно занимаются монетизацией взлома.

ИНСТРУМЕНТЫ

Open-source-утилиты и общедоступные средства тестирования защищенности.

КАК СЕБЯ ПРОЯВЛЯЮТ

Активно сканируют периметр и приложения общедоступными утилитами и инструментами, используют простейший DDoS. Это приводит к перебоям в работе корпоративных сервисов. В случае успешного проникновения в инфраструктуру быстро теряют интерес или обнаруживают себя.

ПРИМЕР ЖЕРТВЫ

Мэрия города с населением 900 тыс. человек

Порядка 90% госструктур уязвимы не только для продвинутых кибергруппировок, но и для злоумышленников с низким уровнем квалификации.

*«Ростелеком-Солар», 2020

КАК ОБНАРУЖИТЬ АТАКУ

Внимательные ИТ-администраторы легко обнаруживают деятельность киберхулиганов по жалобам пользователей на сбои в работе АРМ. Базовые средства защиты фиксируют большинство нелегитимных действий злоумышленников данного уровня.

КАК ОТ НИХ ЗАЩИТИТЬСЯ

- WAF
- UTM
- Patch-менеджмент
- Антивирус
- Анализ журналов аудита СЗИ
- Антиспам

Уровень 3. Кибермошенники

Нацелены на получение прямой финансовой выгоды путем кражи денег, получения выкупа и за счет несанкционированного майнинга. Часто объединяются в организованные группировки.

ИНСТРУМЕНТЫ

Вредоносное ПО и известные уязвимости. Методы социальной инженерии, в том числе массовый фишинг.

КАК СЕБЯ ПРОЯВЛЯЮТ

Используют отработанные методики и хорошо известные приемы. При этом уровень сокрытия у них минимальный: заметают следы в инфраструктуре самыми простейшими способами, например очисткой журнала аудита.

ПРИМЕР ЖЕРТВЫ

Региональное подразделение национального телеком-оператора

18 000 компьютеров
Telecom Argentina были заражены шифровальщиком — пользователи зафиксировали сбои в работе нескольких сайтов. Злоумышленники требовали выкуп в размере 7,5 млн долл.

*ZDNet, 2020

КАК ОБНАРУЖИТЬ АТАКУ

Часто обнаружение происходит по факту нарушения доступности внешних сервисов и внутренних ресурсов. В идеале, присутствие в инфраструктуре определяется с помощью базового мониторинга журналов средств защиты и ИТ-инфраструктуры.

КАК ОТ НИХ ЗАЩИТИТЬСЯ

- UTM
- Антивирус
- Антиспам
- WAF
- SA
- Sandbox
- Сегментация сети
- SOC

Уровень 4. Кибернаемники

Действуют в интересах заказчика (конкурента) либо охотятся за крупной монетизацией, например, за счет продажи базы клиентских данных в даркнете. Объединяются в иерархические группы.

ИНСТРУМЕНТЫ

Самостоятельно разработанные инструменты и собственная инфраструктура; длительный этап разведки, тщательная подготовка и подбор инструментов под конкретную компанию. Приобретают 0-day-уязвимости.

КАК СЕБЯ ПРОЯВЛЯЮТ

Проникают в инфраструктуру с помощью целевого фишинга, через подрядчика или взломанные онлайн-сервисы. Долго и скрытно присутствуют в сети жертвы, скорее всего, будут искать пути попадания в технологические сегменты. Действуют в обход средств защиты, так как предполагают, что в компании осуществляется мониторинг и анализ журналов средств защиты.

ПРИМЕР ЖЕРТВЫ

Крупный федеральный бизнес

Ticketmaster стал жертвой supply chain-атаки, от которой **пострадало 5% клиентов компании.** Источником проблем стало приложение для общения в чате, код которого был модифицирован для кражи данных.

**SecurityLab, 2018

КАК ОБНАРУЖИТЬ АТАКУ

Трудно выявить на этапе проникновения. Детектирование происходит с помощью продвинутой аналитики событий в сети и на хостах. В случае обнаружения на поздних стадиях атаки есть шанс «отбросить» злоумышленника назад, что часто приводит его к отказу от цели.

КАК ОТ НИХ ЗАЩИТИТЬСЯ

- UTM
- Антивирус
- Антиспам
- WAF
- SA
- Sandbox
- Сегментация сети
- NTA
- EDR
- IRP
- СЗИ АСУ ТП
- Anti-APT
- Продвинутый SOC

Уровень 5. Проправительственные группировки

Служат интересам государственных структур и террористических организаций. Ориентированы на перехват полного контроля над инфраструктурой, хактивизм.

ИНСТРУМЕНТЫ

Разрабатывают уникальные техники и тактики под каждую жертву. Применяют уникальные модули ВПО, эксплуатирующие 0-day-уязвимости программного и аппаратного обеспечения.

КАК СЕБЯ ПРОЯВЛЯЮТ

Длительный этап разведки, в том числе с привлечением инсайдеров. Проникновение в инфраструктуру происходит любым доступным способом без ограничений по времени и бюджету атаки. Максимально долго и скрытно присутствуют в инфраструктуре, включая закрытые контуры.

ПРИМЕР ЖЕРТВЫ

Управляющая компания федерального оператора атомной энергетики

Данные 3 млн норвежцев были украдены в результате атаки в 2018 году на национальную медицинскую службу. В Полицейском управлении безопасности Норвегии не исключают, что хакеры действовали по заказу иностранного государства.

ТАСС, 2020

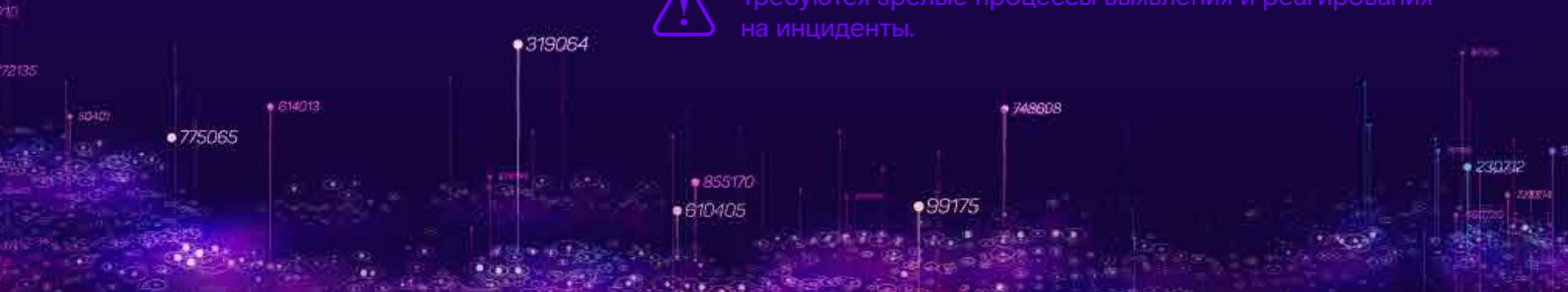
КАК ОБНАРУЖИТЬ АТАКУ

Невозможно выявить на этапе проникновения.
Нацелены на сокрытие действий в сети и на хостах, включая технологический сегмент. В случае обнаружения на поздних стадиях атаки есть шанс «отбросить» противника назад, что не обязательно приведет его отказу от цели, но позволит выиграть время для совершенствования системы защиты.

КАК ОТ НИХ ЗАЩИТИТЬСЯ

- UTM
- Антивирус
- Антиспам
- WAF
- SA
- Sandbox
- Сегментация сети
- NTA
- EDR
- IRP
- СЗИ АСУ ТП
- Anti-APT
- Продвинутый SOC с маппингом по Killchain+Mitre ATT&CK

Требуются зрелые процессы выявления и реагирования на инциденты.



Пройдите тест и узнайте,
какой тип киберзлоумышленника
опасен для вашей организации

О компании «Ростелеком-Солар»

«Ростелеком-Солар», компания группы ПАО «Ростелеком», – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью. В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ.

Solar JSOC компании ПАО «Ростелеком» — первый и крупнейший в России коммерческий центр мониторинга и реагирования на инциденты кибербезопасности (SOC), действующий по модели MDR (Managed Detection and Response).

0.11.BR.AP.01

Ростелеком
Солар

presale@rt-solar.ru rt-solar.ru rt.ru

+7 (499) 755-07-70