Автор: Яков Шпунт

Теги: вирусы, антивирус, аналитик, XDR, MDR, SOC, средства резервного копирования, Linux, Windows, Android

Эволюция защиты от вредоносных программ

Особый эфир AM Live, организованный совместно с Positive Technologies, был посвящён тому, как меняются техники и тактики вирусописателей. Что им могут противопоставить ИБ-специалисты?

Введение 1
Эволюция угроз 2
Классы вредоносов, которые обсуждали аналитики 6
Есть ли безопасные ОС 8
Что противопоставить атакующим 9
Выводы 10

Введение

Использование вредоносных программ стало одним из неотъемлемых элементов атак — и таргетированных, и массовых. В последние годы разномастные вредоносы играют роль всего лишь одного из инструментов в руках злоумышленников, но всё равно занимают значимое место среди угроз как для настольных платформ, так и для мобильных.

Рисунок 1. Участники дискуссии в студии AM Live

В эфир были приглашены:

- **Сергей Голованов**, главный эксперт, «Лаборатория Касперского»;
- **Владимир Нестор**, руководитель группы анализа ВПО центра исследования киберугроз Solar 4RAYS, ГК «Солар»;
- **Теймур Хеирхабаров**, директор департамента мониторинга, реагирования и исследования киберугроз, BI.ZONE.

Ведущий дискуссии — руководитель процессов эмуляции атак и испытания экспертизы продуктов Standoff **Алексей Вишняков** (Positive Technologies).

ВСТАВКА ВИДЕО (https://www.youtube.com/watch?v=jquTL4osQXc)

Эволюция угроз

Как отметили участники дискуссии, что-то принципиально новое среди вредоносного кода если и появляется, то очень нечасто. Это связано с целым рядом факторов.

С одной стороны, сыграло свою роль усиление механизмов защиты операционных систем, которое существенно осложняет работу вирусописателей. С другой — разработка уникального кода дорого стоит, занимает много времени, но при этом вполне может не дать нужного эффекта. Как следствие, злоумышленникам проще перепаковать хорошо известный старый вредоносный код, который доказал свою эффективность, чем писать что-нибудь заново. Поэтому до 90 % всех вредоносных программ, с которыми приходится иметь дело аналитикам, выпущены лет семь назад, а то и раньше.

Руководитель группы анализа ВПО центра исследования киберугроз Solar 4RAYS ГК «Солар» Владимир Нестор

Владимир Нестор:

— В атаках очень много ПО с открытым кодом. Также в последние два года злоумышленники всё чаще размещают платформы управления ботнетами в России. Это связано с тем, что многие компании и госучреждения блокируют весь зарубежный интернет-трафик.

Главный эксперт «Лаборатории Касперского» Сергей Голованов

Сергей Голованов:

— Что-то уникальное и новое — большая редкость. Нам приходится иметь дело всё с теми же семействами зловредов из года в год, многим из них 10 лет и даже больше. Только примерно в 10 % случаев злоумышленники вносят в код какие-то изменения. Однако они используют все новейшие достижения в ИТ: например, активно применяют новые языки программирования. Кроме того, злоумышленники всё более активно идут в российские облачные сервисы.

Директор департамента мониторинга, реагирования и исследования киберугроз BI.ZONE Теймур Хеирхабаров

Теймур Хеирхабаров:

— Вирусописатели активно используют готовые инструменты, не только с открытым кодом, но и коммерческие. Это позволило заметно снизить порог входа на этот рынок. Злоумышленники если и применяют что-то новое, то только средства перепаковки, позволяющие «обмануть» антивирусное ПО. Даже с модификациями кода дело иметь приходится очень нечасто.

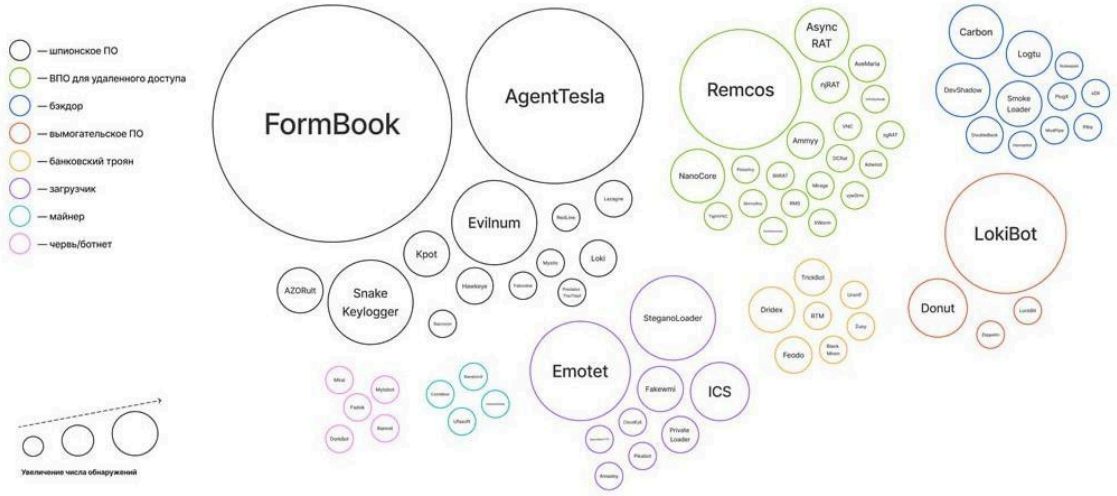
Также хотел бы обратить внимание на то, что вредоносные программы злоумышленники применяют на последней стадии атаки, когда они уже проникли в систему, закрепились там и отключили все средства защиты. На остальных фазах зловреды не используются.

Руководитель процессов эмуляции атак и испытания экспертизы продуктов Standoff Positive Technologies Алексей Вишняков

Алексей Вишняков:

— Многие аналитики жалуются на то, что им изо дня в день приходится изучать одни и те же образцы. Сейчас, как показывает статистика Positive Technologies, большая часть вредоносного кода известна и распространяется уже долгие годы.

Рисунок 2. Основные классы вредоносных программ в России, обнаруженные PT Sandbox



Классы вредоносов, которые обсуждали аналитики

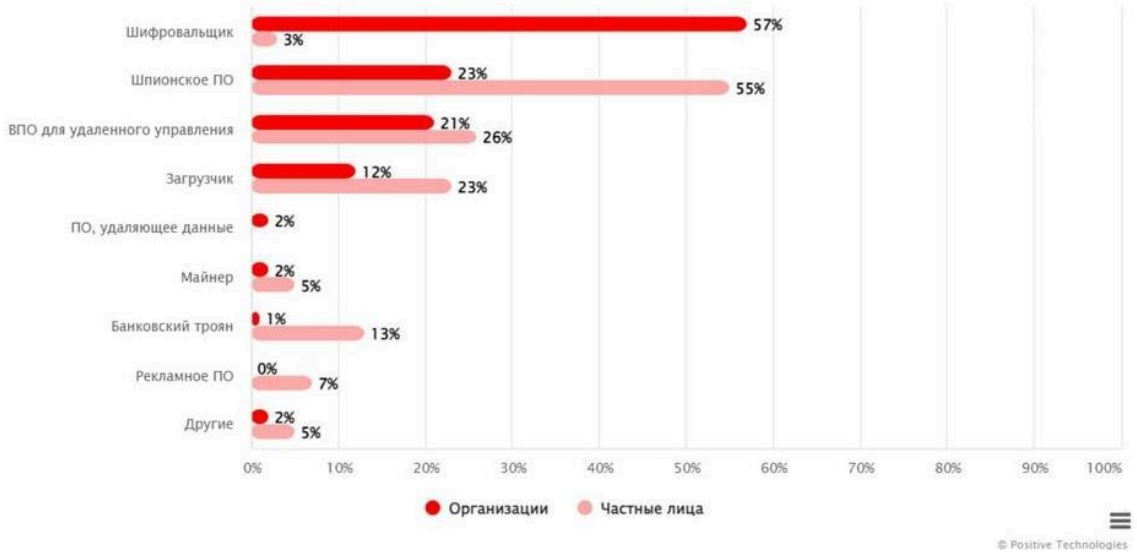
Обсуждение резонансных технологий участники дискуссии начали с бесфайловых вирусов, которые в своё время наделали много шума. По мнению Сергея Голованова, эти вредоносы вызвали широкий резонанс за счёт «эффекта полтергейста», когда в системе происходит вредоносная активность, но возникает она словно ниоткуда. Представитель «Лаборатории Касперского» назвал такие вирусы весьма давней угрозой (они существуют уже около 15 лет), но в реальной практике редкой.

Теймур Хеирхабаров связал редкость таких вредоносных объектов со сложностью их разработки и с появлением новых механизмов самозащиты в основных операционных системах. В итоге маскировать их всё сложнее.

Владимир Нестор обратил внимание на то, что такого рода вирусы работают до первой перезагрузки, что делает их непригодными для длительных атак и закрепления в системе. По его оценке, для заражения пригодны только серверы с длительным аптаймом, которые ещё надо найти, что усложняет задачу злоумышленников.

Другим «популярным» классом вредоносных программ стали шифровальщики (рис. 3). При этом, как отметил Алексей Вишняков, они весьма успешно определяются средствами защиты, однако атаки всё равно случаются и наносят значительный ущерб.

Рисунок 3. Основные типы вредоносных программ, которые атаковали российских частных лиц и компании, по итогам 2023 г.



Теймур Хеирхабаров напомнил, что запуск вредоносных программ обычно является последней стадией атаки, когда средства защиты, в том числе

антивирусной, злоумышленники отключили. Если процесс работы шифровальщика уже начался, то счёт идёт на минуты, если не на секунды.

Сергей Голованов добавил, что помимо антивирусного ПО хакеры отключают средства резервного копирования, попутно удаляя уже сделанные резервные копии. При этом злоумышленники всё чаще атакуют на уровне хостов виртуальных машин, а не каждой системы в отдельности. В итоге остаётся меньше времени на то, чтобы отразить атаку.

С другой стороны, как отметил Сергей Голованов, часто злоумышленники не особенно утруждают себя и, например, используют неуникальные ключи либо шифруют не весь диск, физический или виртуальный, а лишь его часть, причём относительно небольшую. В итоге данные удаётся восстановить.

Другим классом вредоносных объектов, появление которых вызвало широкий резонанс в отрасли, стали буткиты. Однако, как вспоминает Алексей Вишняков, они исчезли так же быстро, как и появились. Сергей Новиков связал это с тем, что данный класс вредоносов использовал недокументированные функции операционных систем и требовал от вирусописателя высокой квалификации. С появлением в 2017 г. буткита с открытым кодом, исходный текст которого появился тогда в одном из репозиториев, их научились успешно детектировать антивирусные средства. После этого, как заявил представитель антивирусного вендора, такие вредоносы и исчезли.

А вот руткиты, как предупредил Теймур Хеирхабаров, являются вполне типичными для платформы Linux, хотя для Windows они — пока редкость. По оценке представителя BI.ZONE, этот класс вредоносных программ дорог и требует высокой квалификации разработчика. Вместе с тем он широко востребован в атаках. Как обратил внимание Владимир Нестор, именно с помощью руткитов злоумышленники отключают средства защиты. При этом, по словам Сергея Голованова, применение таких инструментов не всегда легко обнаружить.

Первый опрос в ходе эфира был посвящён тому, кто занимается исследованием вредоносных программ в компаниях (рис. 4). Его результат оказался для участников дискуссии неожиданным, поскольку каждый пятый зритель заявил о том, что в компании, где он работает, имеются вирусные аналитики. По единодушному мнению экспертов, наличие вирусных аналитиков — большая редкость даже для крупных компаний в России.

Рисунок 4. Есть ли в вашей компании выделенный специалист по расследованию инцидентов связанных со вредоносными программами?

Есть ли безопасные ОС

По мнению Владимира Нестора, безопасной можно считать ту операционную систему, у которой мала пользовательская база. Он привёл в пример Linux, которая была практически абсолютно безопасной тогда, когда ею пользовались исключительно энтузиасты — но когда аудитория выросла, начались атаки, причём они проходили по вполне стандартным схемам.

Теймур Хеирхабаров назвал эту ситуацию естественной: по мере роста пользовательской базы становятся видны недостатки той или иной системы, которые потенциальный злоумышленник может использовать для атаки.

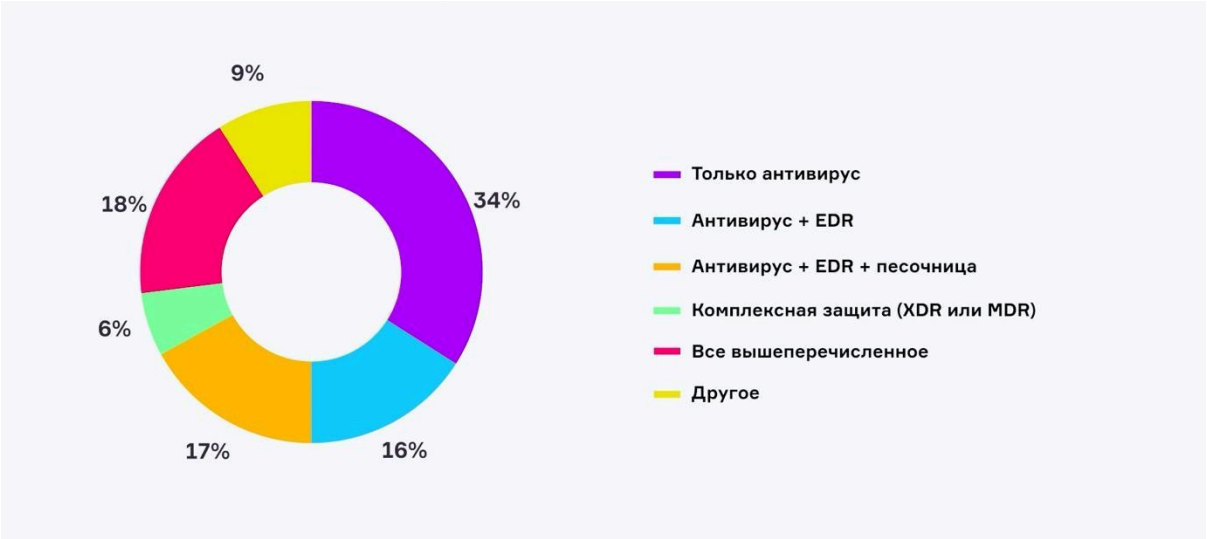
По мнению Сергея Голованова, одно лишь наличие средств разработки делает возможным написание вредоносных программ для любой платформы. По его мнению, определённым препятствием может стать лишь установка ПО через жёстко контролируемый владельцем платформы официальный магазин приложений — и даже эта преграда, как показывает практика, преодолима для вирусописателей.

Теймур Хеирхабаров назвал лазейкой возможность подмены разделяемых библиотек. Он напомнил, что существуют образцы подобных вредоносов для разных платформ, причём основной исполняемый файл может иметь все нужные подписи.

Сергей Голованов уточнил, что спецификой атак на Linux часто является подмена репозиториев, особенно когда системы используют DEB-пакеты (Debian, Ubuntu и их производные). Спецификой атак на мобильные платформы, особенно если необходимо перехватить какую-то важную информацию, является, как отметил представитель «Лаборатории Касперского», использование функции трансляции экрана в ряде приложений, в частности — во многих популярных мессенджерах. Именно так злоумышленники перехватывают коды из СМС-сообщений.

Второй опрос зрителей был посвящён тому, какие средства используются в их компаниях для борьбы со вредоносными программами (рис. 5). По мнению экспертов, его результаты показывают, что компании начинают осознавать недостаточность использования базовых средств защиты.

Рисунок 5. Какие средства защиты от вредоносных программ используются в вашей компании?



Что противопоставить атакующим

Прежде всего, антивирусные аналитики и разработчики антивирусного ПО активно применяют новые технологии. Так, они задолго до бума последних двух лет использовали искусственный интеллект и машинное обучение. С появлением генеративного ИИ и больших языковых моделей, как отметил Владимир Нестор, стало проще проводить реверс-инжиниринг образцов кода: достаточно скопировать фрагмент, и нейросеть определит, к какому семейству относится вредонос. Однако, как предупредил представитель ГК «Солар», это работает только для распространённых типичных образцов.

Как отметил Алексей Вишняков, уже через 1,5 месяца начинающие специалисты начинают определять основные образцы вредоносного кода с помощью баз из открытых источников без использования реверс-инжиниринга.

Теймур Хеирхабаров назвал машинное обучение давно и широко используемым инструментом создания сигнатур, в том числе для антивирусного ПО. К нему прибегают, по его словам, все без исключения вендоры, причём уже очень давно. Применяется машинное обучение и для защиты конечных точек. Тут по-прежнему есть много ограничений, однако от целого ряда актуальных угроз, например шифровальщиков, такие инструменты хорошо помогают.

Как подчеркнул Сергей Голованов, машинное обучение полезно антивирусным вендорам тем, что механизмы его работы непонятны посторонним, в том числе и

злоумышленникам, которые не прочь нарушить деятельность разработчиков средств защиты. Однако, по его оценке, в ближайшей перспективе в этой сфере ничего принципиально нового не появится.

Теймур Хеирхабаров считает, что аналитик — это «штучный товар», которого пока ничто не может заменить, тем более что такой специалист, как правило, умеет определять и другие угрозы, а не только вредоносные программы. В конце концов, целью ИБ является защита от атак, а не от отдельных их элементов.

Владимир Нестор добавил к этому, что нужно не только строить защиту, но и тщательно анализировать все инциденты и понимать их причины, чтобы потом не допустить повторения. Сергей Голованов назвал анализ вредоносных программ важной частью построения системы защиты.

Завершающий опрос (рис. 6) был посвящён тому, считают ли зрители необходимым проводить анализ вредоносного кода. Эксперты назвали полученные результаты вполне ожидаемыми: три четверти опрошенных говорят, что делать это нужно, но не у всех есть необходимые ресурсы. Теймур Хеирхабаров обратил внимание на то, что не каждый образец требует исследования: по большей части для получения полезных результатов достаточно данных от мультисканера.

Рисунок 6. Нужно ли проводить анализ вредоносного кода в рамках расследования инцидентов?

Выводы

Применение вредоносных программ является одним из элементов атак на обычных пользователей и компании. Его развитие несколько замедлилось в последние 10 лет, но не прекратилось. Вирусописатели успешно адаптируются

как к усовершенствованным механизмам самозащиты операционных систем, так и ко внешним средствам обеспечения ИБ.

Решения для проактивной защиты от вредоносного кода, такие как песочницы, совершенствуют возможности по детектированию современных угроз. Для того чтобы узнать, как справляется с защитой бизнеса от атак с использованием вредоносов песочница от Positive Technologies — PT Sandbox, регистрируйтесь на митап NetCase Day от Positive Technologies, который пройдёт 24 сентября в 16:00. На мероприятии реальные пользователи поделятся честными историями о PT Sandbox и PT NAD.

Реклама, АО «Позитив Текнолоджиз», 7708668887

ERID: 2Vfnxxawf7n

Телепроект AM Live еженедельно приглашает экспертов отрасли в студию, чтобы обсудить актуальные темы российского рынка ИБ и ИТ. Будьте в курсе трендов и важных событий! Для этого подпишитесь на наш канал в YouTube.