



POSITIVE TECH PRESS CLUB

**Вредоносное ПО.
Топ угроз и технологии
защиты**



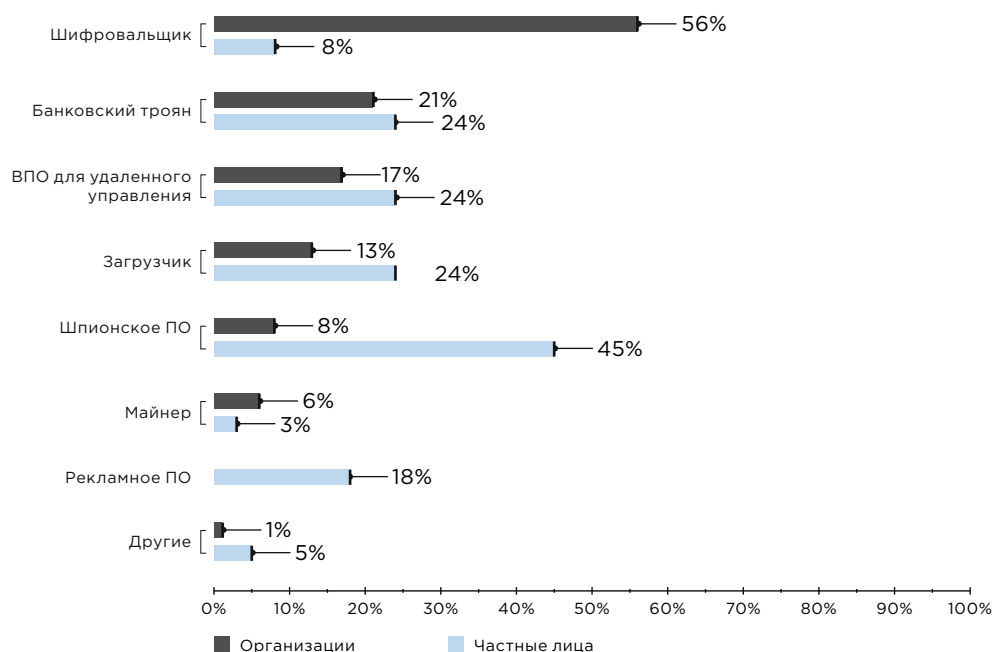
Алексей Вишняков

Руководитель
отдела обнаружения
вредоносного ПО
экспертного центра
безопасности Positive
Technologies (PT Expert
Security Center)

Ландшафт угроз вредоносного ПО: тренды и прогнозы

Шифровальщики и шпионское ПО в авангарде атак

Лидером 2020 года по количеству атак стали операторы программ-вымогателей. Доля таких атак составила 56% среди всех инцидентов с использованием вредоносного ПО (ВПО) и нацеленных на юридических лиц. В атаках на частных лиц на первом месте находится шпионское ПО, его доля среди инцидентов с использованием ВПО составила 45%.



© Positive Technologies

Рисунок 1. Типы вредоносного ПО (доля атак с использованием вредоносного ПО)

Атлас вредоносного ПО



Шифровальщик — вредоносная программа, которая шифрует содержимое чувствительных данных пользователя ПК. Жертве предлагается заплатить выкуп за восстановление данных. В последнее время стало актуальным так называемое двойное вымогательство: перед зашифровкой данные передаются на сервер злоумышленника, в следствие чего пользователь получает угрозы о публикации данных, если выкуп не будет выплачен.



Шпионское ПО — вредоносная программа, которая следит за пользователем и крадет конфиденциальную информацию: записывает нажатые клавиши клавиатуры и мыши, делает снимки экрана, извлекает учетные данные пользователя из браузеров, почтовых клиентов, мессенджеров и прочих конфигурационных файлов, выполняет аудиозапись микрофона или видеозапись с веб-камеры.



ВПО для удаленного управления — вредоносная программа, обеспечивающая полный контроль над зараженной машиной. Предназначена для выполнения произвольного кода атакующего. Этот класс ВПО является связующим звеном для других узконаправленных образцов ВПО.



Загрузчик — вредоносная программа, загружающая и запускающая другое дополнительное ВПО по сети. Используется для получения первичной информации о пользователе: имя пользователя, имя компьютера, версия операционной системы, IP-адрес и т. д. Наиболее часто применяемый вид ВПО на первых этапах атаки.



Банковский троян — вредоносная программа, нацеленная на кражу финансовой информации. ВПО этого класса может извлекать номера банковских карт пользователя, перехватывать учетные записи для доступа в личный кабинет банка, получать адреса криптокошельков из буфера обмена. Банковские трояны скрываются в браузерных процессах, чтобы не выдать свои действия.



Майнер — вредоносная программа, нацеленная на выработку криптовалюты за счет ресурсов ПК пользователя. ВПО злоупотребляет процессорными возможностями и производительностью видеокарты. Часто используется для монетизации проводимых атак.



Рекламное ПО — не вредоносная программа, выполняющая монетизацию для оператора за счет отображения информации рекламного характера. Поставляется в составе установщиков другого ПО (bundle), вместе с вредоносным ПО либо в качестве расширений в браузере. Нередко привлекает внимание пользователя нежелательными всплывающими окнами, подписками и кликами в интернете.

Доля шифровальщиков среди прочего ВПО, замеченного в атаках на юридических лиц, в 2020 году увеличивалась с каждым кварталом, в IV квартале достигнута точка максимума за 2020 год — 56% инцидентов с ВПО были совершены с применением программ-вымогателей.

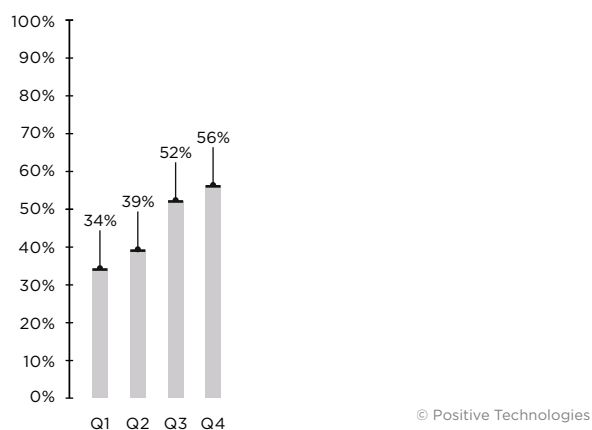


Рисунок 2. Доли атак с использованием шифровальщиков среди всех атак на юридических лиц, реализованных с помощью ВПО

Больше всего операторов программ-вымогателей интересуют медицинские (20%) и государственные учреждения (19%), а также предприятия промышленности (11%).



Рисунок 3. Жертвы шифровальщиков среди юридических лиц

Также шифровальщики задали тренд на увеличение сумм выкупов. Сейчас они не просто шифруют сеть компании, но еще и крадут конфиденциальные данные. Таким образом у жертв появляются целых два повода заплатить запрашиваемую злоумышленниками сумму: чтобы не только получить дешифровщик и быстрее восстановить работоспособность компании, но и предотвратить распространение важных для компании сведений.

Способы доставки вредоносов

В атаках на юридических лиц для доставки ВПО злоумышленники по-прежнему чаще всего используют электронную почту (65%). Со II квартала 2020 года был замечен тренд на переход к компрометации ресурсов сетевого периметра: хакеры стремятся найти уязвимости на сетевом периметре организаций, изучая слабые места в необновленных VPN-решениях и эксплуатируя бреши в веб-приложениях компаний. Так, например, сделали и операторы программы-вымогателя Netwalker.

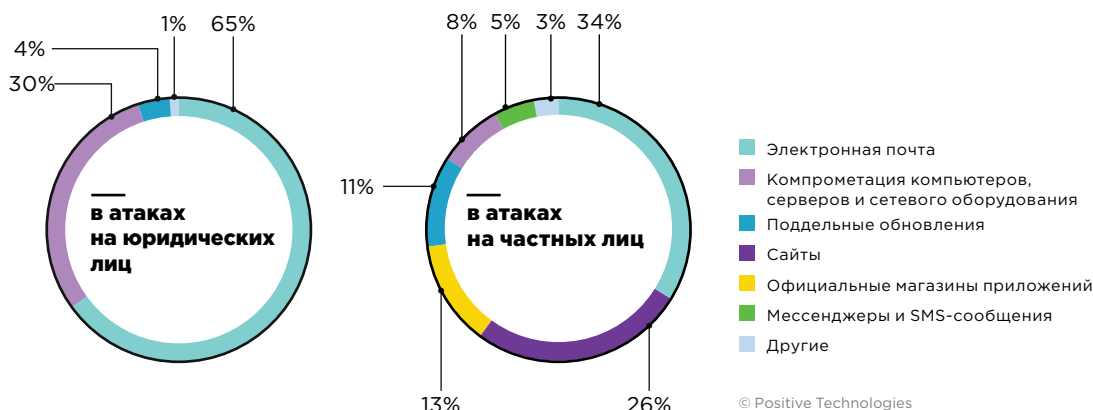


Рисунок 4. Способы распространения вредоносного ПО

В атаках на частных лиц для доставки ВПО по-прежнему чаще всего используются электронная почта (34%) и сайты (26%).

Что нужно знать о развитии ВПО: прогнозы

- В 2021 году самым распространенным способом доставки ВПО на устройства и в сеть жертвы останется фишинг, реже атакующие будут прибегать к компрометации сетей путем подбора слабых паролей на RDP-серверах или эксплуатации уязвимостей в веб-серверах.

Рекомендации: Защита конечных точек антивирусными решениями, использование продуктов класса песочницы, межсетевых экранов уровня веб-приложений и многофакторной аутентификации.

- Вымогательское ПО останется в авангарде атак с применением ВПО. Злоумышленники все чаще будут прибегать к двойной схеме вымогательства: шифрованию файлов и шантажу публикацией украденной информации в сети. О таких случаях мы слышим все чаще. Среди недавних примеров атак с двойным вымогательством отмечены случаи с [HelloKitty](#): [CD Projekt](#), [Cyberpunk 2077](#), [DoppelPaymer](#); [Kia Motors](#), [Clon](#); [Bombardier](#), [Conti](#); [SEPA](#). Мы наблюдаем высокую активность таких вымогателей, как Egregor (атаковано около 150 компаний, суммарные убытки достигают 80 млн долларов), [Ryuk](#) (один из ярких примеров — ущерб, нанесенный компании Universal Health Services (UHS), в размере 67 млн долларов), Thanos, Ragnar.

Рекомендации: Регулярное резервное копирование ценной информации, контроль критичных узлов внутренней инфраструктуры, игнорирование требований вымогателей.

- Продолжат свое развитие и истории с атаками на компании через цепочку поставок¹. Только за последнее время были зафиксированы случаи с [SolarWinds](#), [Centreon](#), [ANSSI](#), [NightScout](#), [SignSight](#), [Vietnamese government](#), [StealthyTrident](#), [Able Desktop](#), [Mongolia](#), [WIZVERA](#) VeraPort, [South Korea](#), [СНБО](#). Еще один из примеров, сравнимый по масштабам и последствиям с нашумевшим взломом SolarWinds, — атака на французскую компанию Centreon, предоставляющую ПО для мониторинга корпоративных сетей. Операция группировки длилась три года. Среди пострадавших клиентов Centreon оказались Airbus, Air France KLM, Agence France-Presse (AFP), Euronews, Orange, Arcelor Mittal, Sephora, министерство юстиции Франции.

Рекомендации: Контроль аномалий поведения ПО, централизованный анализ событий в корпоративной инфраструктуре, совершенствование процессов реагирования на инциденты.

- Спрос на доступ к взломанным компаниям продолжит расти. По данным [Positive Technologies](#), в 90% случаев в дарквебе на форумах, посвященных взлому сайтов, ищут хакера, который сможет предоставить заказчику доступ к ресурсу или выгрузит базу пользователей. В 7% записей фигурируют предложения услуг по взлому сайтов. Остальные сообщения направлены на продвижение сервисов и программ для взлома веб-приложений и поиск единомышленников по взлому.

Рекомендации: Своевременное обновление ПО на периметре организации, построение процесса проактивного поиска угроз (Threat Hunting).

- Продолжатся атаки на промышленные объекты и АСУ ТП. Например, одним из недавних случаев стал [инцидент в городе Олдсмар](#), штат Флорида. Неизвестные киберпреступники смогли проникнуть в компьютерные системы, управляющие водоочистными сооружениями. В результате злоумышленники смогли удаленно контролировать химический состав воды.

Рекомендации: Должное внимание к защите не только корпоративного, но и технологического сегмента сети.

- Будут совершенствоваться возможности операций вымогателей в части закрепления в прошивках (BIOS/UEFI) и распространения внутри сети, что усложняет удаление ВПО и увеличивает количество пострадавших рабочих станций.

Рекомендации: Контроль полномочий учетных записей пользователей, своевременное обновление ОС.

¹ Суть атаки следующая: атакующий не компрометирует компанию А, вместо этого компрометируется компания В. Ввиду того, что компании А и В — партнеры, выступают в роли заказчика-клиента, например ПО от компании В поставляется в компанию А, или связаны как-то иначе. В итоге скомпрометированное ПО компании В попадает в компанию А, что приводит к компрометации последней.

- Злоумышленники продолжают искать способы скрыть свое присутствие и оставаться как можно дольше незамеченными в сети жертвы. Для этого они добавляют новые функции в свои вредоносы, например проверку среды запуска. В случае, если ВПО запущено на виртуальной машине, вредоносные модули не активируются. Наше [исследование](#) показало, что в 56% изученного ВПО для удаленного доступа и в 14% исследованных загрузчиков использовались техники обхода песочниц и защита от обнаружения средствами анализа кода. В остальных типах ВПО такие техники встречаются реже.

Рекомендации: Кастомизация образов решений класса песочницы, проактивный анализ поведения программ на конечных станциях пользователей.

- Могут получить развитие случаи с появлением вредоносного ПО на языке IronPython (уже известны [два таких случая](#)) и малварью Silver Sparrow, разработанной под новые процессоры Apple M1: теперь операторы портируют ВПО не только под разные кодовые платформы, но и архитектуры процессоров.

Рекомендации: Внимание к защите не только широко распространенных, но и прочих операционных систем (Linux, MacOS и др.), если они используются в компании.

Наиболее активные вредоносы

СЕМЕЙСТВО	ПРОИСХОЖДЕНИЕ	ОСОБЕННОСТЬ
NjRAT	Средний Восток	Исходный код доступен в сети
FormBook	Россия/СНГ	Инфостилер ² по схеме Malware-as-a-Service
AgentTesla	Турция	Экспфильтрация ³ данных через почтовый протокол
LokiBot	Россия/СНГ	Один из крупнейших ботнетов
NanoCore	США	Продается как легитимный инструмент для удаленного администрирования
Remcos	Россия/СНГ	Часто используется атакующими из средневосточного региона
QuasarRAT	Н/д	Исходный код доступен в сети, используется азиатскими группировками, код сильно обфусцирован ⁴
Masslogger	Н/д	Код сильно обфусцирован, проверяет наличие антивирусов в системе

2 ПО для кражи информации.
3 Извлечение, передача данных.
4 Усложнение кода для анализа.

СЕМЕЙСТВО	ПРОИСХОЖДЕНИЕ	ОСОБЕННОСТЬ
QBot	Н/д	Основные цели - компании в США, многомодульная архитектура для расширения возможностей
<u>Minebridge</u>	Россия/СНГ	Используется русскоязычной группировкой <u>TA505</u> , многослойная упаковка исполняемого кода для усложнения анализа

Наиболее активные АРТ⁵-группировки

ГРУППА	ПРОИСХОЖДЕНИЕ	МОТИВАЦИЯ	ЧИСЛО АТАК ⁶ В Q4 2020 ГОДА
Gamaredon	Украина	Шпионаж	
APT31	Китай	Шпионаж	
APT32	Вьетнам	Шпионаж	
Lazarus	Северная Корея	Финансы + Шпионаж	2 атаки
LazyScripter	Н/д	Н/д	
Sandworm	Россия	Шпионаж	
Turla	Россия	Шпионаж	
RTM	Россия	Финансы	51 атака
CloudAtlas (PowerShower)	Н/д	Шпионаж	3 атаки
Winnti (Bisonal)	Китай	Финансы + Шпионаж	2 атаки
TA428 (RoyalRoad и NccTrojan)	Китай	Шпионаж	2 атаки

Операторы вымогательского ПО регулярно вносят в него изменения и придумывают все новые подходы к атакам. Особенно сильно в этом преуспели АРТ-группировки. Чтобы противостоять угрозе, необходимо выстроить эффективный цикл обновления и патчинга применяемого в компании программного обеспечения, защищать сетевой периметр, уделять особое внимание безопасности учетных записей и использовать многофакторную аутентификацию. Чтобы иметь возможность выявлять ВПО на всех стадиях атаки, необходимы современные решения класса песочницы, систем обнаружения вторжений, сбора и мониторинга событий информационной безопасности, а также автоматизации реагирования на инциденты.

5 Advanced persistent threat, то есть «целевая кибератака».

6 Число атак группы, зафиксированное PT Expert Security Center. Данные представлены только по тем группам, которые на данный момент исследуются PT Expert Security Center.



Алексей Данилин

Руководитель направления
по развитию бизнеса,
Positive Technologies

В 31% атак

на российские компании
было замечено ВПО;

25% вредоносных программ

были активны
в 2019–2020 годах.

Исследование Positive Technologies «[Обнаружение и обход песочниц. Как изменилось вредоносное ПО за 10 лет](#)»

Песочница (sandbox)

запускает файл в изолированной виртуальной среде, анализирует действия, которые он совершает в системе, и выдает вердикт о том, безопасен этот файл или нет.

Песочницы сегодня: рынок и пользователи

По нашей статистике, самые распространенные атаки на информационную инфраструктуру — те, что используют вредоносные программы. Среди различных типов ВПО в атаках на компании лидируют шифровальщики (56%), банковские трояны (21%) и ВПО для удаленного управления (17%), а в атаках на частных лиц — шпионское ВПО (45%), банковские трояны (24%), ВПО для удаленного управления (24%) и загрузчики (24%). При этом вредоносное ПО применяется и в атаках, направленных на конкретные предприятия: такой целевой характер носят 8 из 10 зарегистрированных нами инцидентов.

Что такое песочницы

Создатели вредоносного ПО постоянно развивают свои инструменты: встраивают функции выявления и обхода средств защиты и придумывают новые техники, минимизирующие вероятность обнаружения ВПО по известным индикаторам компрометации (indicators of compromise, IOC). Злоумышленники зачастую могут обойти антивирусы, шлюзы безопасности и IDS⁷/IPS⁸. Там, где с атаками не справляются базовые средства защиты, на помощь приходят песочницы.

Песочницы способны выявлять неизвестные ранее угрозы — те, которые еще не встречались классическим средствам защиты.

История песочниц

Первые песочницы появились на российском рынке защиты от атак с применением ВПО более 8 лет назад. Сегодня на нем представлены как отечественные, так и зарубежные решения. За это время вендоры успели пройти большой путь — им необходимо было создать эффективные способы не позволить ВПО понять, что оно попало в виртуальную среду, а также решить задачи, связанные с производительностью и непрерывностью бизнес-процессов (например, настройкой почты «в разрыв»), и обеспечить интеграцию с другими IT- и ИБ-системами.

В каких отраслях востребованы песочницы

Песочницы используют компании, в которых уровень зрелости ИБ выше среднего. Эти организации как минимум уже обзавелись базовыми средствами безопасности и задумались о защите от целевых атак, а как максимум — организовали свои центры реагирования на киберугрозы (security operation center, SOC).

⁷ Intrusion Detection System — система обнаружения вторжений.

⁸ Intrusion Prevention System — система предотвращения вторжений.

В настоящее время среди основных пользователей песочниц можно отметить:

- **Государственные организации.** В этом сегменте исторически делался упор на соответствие требованиям регуляторов и так называемую бумажную безопасность, но в прошедший карантинный год этим учреждениям пришлось переходить на удаленную работу, и некоторые из них пострадали от ВПО. Так, в конце 2020 года государственные учреждения были на верхних строках рейтинга жертв программ-вымогателей — чаще других оказывались под прицелом операторов шифровальщиков (19%), уступая только медицинским организациям (20%).
- **Промышленность.** Результаты проведенного анализа киберугроз подтверждают, что вредоносное ПО применяется в 84% атак на промышленные объекты. Злоумышленники все чаще пытаются скомпрометировать инфраструктуру предприятий, в том числе через целенаправленные атаки на технологический сегмент (АСУ ТП⁹). Преступники продают и покупают в дарквебе доступы к внутренним сетям предприятий, останавливают работу промышленных объектов, а затем требуют выкуп за расшифровку данных и неразглашение похищенной информации.
- **Логистика и ритейл.** По данным Data Insight, рынок e-commerce в 2020 году вырос на 44%. По оценке аналитиков, не случись пандемия, рост этого рынка составил бы только 29%. Компании в этом сегмента стали более привлекательны для злоумышленников. Наши исследования подтверждают, что количество атак на отрасль торговли достигло абсолютного максимума за последние два года: число инцидентов в IV квартале 2020 года увеличилось на 77% по отношению к аналогичному периоду 2019-го. Чаще всего злоумышленники похищают данные (платежных карт, персональные данные, учетные), в 31% инцидентов в этой сфере задействованы программы-вымогатели.
- **Медицинские учреждения.** Целями злоумышленников все чаще становятся клиники, лаборатории по разработке вакцин, фармацевтические компании. Не последнюю роль в этом сыграла пандемия COVID-19. Проведенный нами анализ киберугроз в последнем квартале 2020 года показал, что операторы шифровальщиков чаще всего атаковали именно медучреждения (20%). Преступников интересуют данные о разработке новых препаратов, в том числе вакцин, результаты клинических испытаний и персональные данные пациентов.
- **Финансовые учреждения.** Кредитно-финансовая сфера традиционно считается одной из самых защищенных, но инциденты в этой отрасли все равно происходят. В IV квартале 2020 года 6% всех жертв атак пришлось на финансовые организации.

Тем не менее одним из самых распространенных методов доставки ВПО по-прежнему остается фишинг (65% в атаках на организации), поэтому компрометация возможна в любой компании, где используется электронная почта, независимо от отрасли.

Какие задачи решают песочницы

При выборе песочниц пользователи в первую очередь ожидают получить вместе с продуктом экспертизу (что позволит уменьшить требования к специалистам по ее эксплуатации), возможности легкой интеграции с другими внешними и внутренними системами (запрос на экосистему решений), а также качество детектирования.

В марте мы провели опрос, в котором приняли участие более 100 компаний, уже использующих песочницы, из различных отраслей. Выяснилось, что самые популярные задачи, которые решают с помощью песочниц, — это проверка файлов из интернета (64%), ручные проверки (57%) и проверка электронной почты (54%).

Также мы просили респондентов указать, какой функционал песочниц они определяют как самый важный. В число самых популярных ответов вошла возможность имитации реальных рабочих станций с помощью гибкой настройки (кастомизации) виртуальных сред и размещения приманок (за нее проголосовали 46% опрошенных).

Как работает кастомизация виртуальных сред? В общем смысле она позволяет добавлять в песочницу, где анализируется файл, программное обеспечение, которым пользуются сотрудники в компании, то есть максимально точно имитировать реальную инфраструктуру. С помощью кастомизации песочница может выявлять атаки, использующие конкретное приложение или даже определенную его версию, а также обнаруживать угрозы нулевого дня. Например, если атака направлена на эксплуатацию уязвимости в Foxit Reader, который используют в компании, а в виртуальной среде по умолчанию установлен Adobe Acrobat Reader, песочница без кастомизации пропустит угрозу.

Предложение для этого запроса на рынке почти отсутствует — таких систем практически нет, и мы стремимся закрыть этот разрыв своими технологиями.

Что изменится на рынке песочниц в ближайшие 2–3 года

Сейчас, почти десятилетие спустя, песочницы еще не достигли потолка своего развития с точки зрения технологий детектирования атак. Постоянное усложнение угроз и рост числа целевых кампаний требует от песочниц гибкости — эти системы должны учитывать специфику инфраструктуры компании, особенности индустрии, географию. Для эффективного выявления угроз необходимо создавать реалистичную виртуальную среду, максимально приближенную к существующей инфраструктуре конкретной компании.

Исходя из этого, наша цель — обеспечить эффективную персонализированную защиту бизнеса с учетом его ключевых рисков. Главный инструмент для достижения этой цели — гибкая настройка, кастомизация виртуальных сред, а также внедрение в песочницы deception-технологий, «приманок» для злоумышленников. Мы отмечаем интерес к кастомизации виртуальных сред на пилотных проектах, его подтверждают наши исследования и опросы, поэтому мы предполагаем, что данный подход станет трендовым и превратится в устойчивый клиентский запрос.

Кроме того, выявление целевых атак требует от вендора комплексных экспертных знаний: для глубокого понимания техник злоумышленников необходим опыт, во-первых, в области анализа защищенности, во-вторых, в сфере мониторинга, реагирования и расследования киберинцидентов, а в-третьих, свежие данные по отдельно исследуемым угрозам. Мы регулярно пополняем базу знаний в нашем продукте, чтобы предлагать компаниям защиту, релевантную для ландшафта угроз в России.

Мы предполагаем, что в ближайшие 2 года на отечественном рынке останется лишь несколько конкурентных предложений в данной области. При этом самые распространенные требования бизнеса поделятся на две категории. Одни компании будут делать выбор в пользу оптимизации ресурсов без гарантий полной защиты от атак. Другие же — те, кто осознает риски или уже столкнулся с последствиями целевых кампаний, — выберут решения, в которых сделан упор на персонализацию защиты и экспертные знания. Как вендор, мы видим будущее за решениями из второй группы.



Денис Кораблев

Директор по продуктам,
Positive Technologies

Технологические тренды развития песочниц

Мы видим несколько ключевых направлений, в которых должны развиваться технологии песочниц в ближайшие 3-5 лет, чтобы успешно справляться с возникающими угрозами.

Расширение покрытия модели угроз

Один из наиболее распространенных методов атак, наряду с применением вредоносных программ, — социальная инженерия (50% атак на организации, 86% — на частных лиц). В большинстве случаев злоумышленники сочетают эти методы и используют как ключевой вектор проникновения электронную почту.

Текущий подход к анализу происходящего в электронной почте, как правило, подразумевает проверку файлов и ссылок, а также поиск в теле сообщений паролей для работы с архивами. Однако в этом случае не учитывается часть информации, потенциально выдающей угрозу, — заголовки писем.

По ним можно сразу определить «злонамеренность» сообщения. Например, в заголовках серии Received содержится фактическая информация, которую добавляют почтовые серверы при пересылке письма, и там же часто видны попытки фальсификации адресов отправителя. Кроме того, на основании ранее обнаруженных индикаторов (программа-почтовик, создавшая письмо, идентификаторы письма, адреса промежуточных узлов пересылки) можно отнести ту или иную рассылку к злонамеренной.

Сейчас заголовки анализируют в основном решения другого класса — антиспам-системы. Однако важно понимать, что задача защиты от спама лишь частично пересекается с более серьезной проблемой защиты от целевых атак, которую призваны решать песочницы. Для более полного покрытия модели угроз песочницам необходимо выполнять и эту функцию.

Производительность: «стеклянный потолок»

Производительность до сих пор является одним из ключевых параметров, на которые обращает внимание пользователь при выборе песочницы. Это подтверждают и результаты нашего опроса, в котором приняли участие представители более 100 компаний, уже применяющих такие технологии. Сейчас заказчики, как правило, воспринимают песочницы как инструмент предотвращения угроз и хотят стопроцентной изоляции потенциально опасного файла до попадания в сеть. В этом случае время проверки составляет в среднем 1-2 минуты на каждый файл.

Это привело к тому, что возник некий негласный потолок возможной производительности — и с точки зрения времени, и с точки зрения стоимости. Пока эту задачу частично решает предварительная фильтрация с помощью статического анализа, но эта технология заточена только на поиск простых и известных угроз и не способна выявить инструменты для целевой атаки.

На самом деле производительность песочниц все еще можно развить в сторону ускорения и удешевления без потери качества. Один из возможных путей: массовая единовременная проверка больших наборов файлов по косвенным признакам: попыткам закрепиться в системе, подключиться к интернету и т. д. Если такие признаки обнаружатся, песочница может проводить дополнительную проверку — и, напротив, пропускать файлы, не совершающие подозрительных действий. Как выделить оптимальные косвенные признаки, которые позволят не пропустить угрозу, — вопрос, который только предстоит решить.

Работа с реальными рисками и персонализация защиты

Выстраивание корпоративной безопасности должно зависеть от того, какие риски компания считает приоритетными для себя. ИБ-продукты, с помощью которых планируется решать эту задачу, должны быть достаточно гибкими, чтобы обеспечивать персонализированную защиту. Почему? Дело в том, что подавляющее большинство атак — 80% — целевые. Злоумышленники стремятся узнать о жертве как можно больше и на основе этих знаний выбирают готовые инструменты для атаки или разрабатывают их с нуля. Очевидно, что в подобных условиях не может быть универсальных решений на все случаи жизни и необходимо отталкиваться от собственной уникальной карты рисков.

Как можно персонализировать защиту? В случае с песочницами наиболее эффективный путь — кастомизировать виртуальные среды и приближать их состав к реальным рабочим станциям. Например, размещать в песочнице те приложения, которые действительно используют сотрудники, вместо программ по умолчанию, а также воссоздавать процессы и файлы, которые свойственны «живой» инфраструктуре. Это поможет спровоцировать атакующих проявить себя на имитации рабочей среды и не дать им добраться до реальной инфраструктуры, а значит, извлечь из продукта максимальную пользу и нивелировать угрозы, направленные на критически важные для бизнеса системы.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте ptsecurity.com.