pandasecurity.com/business/

Отчет Понимание угроз 2020

panda

Отчет Panda Security "Понимание угроз 2020"

Уведомление о правах

Содержание :

panda

| Краткий обзор

В условиях распространения и постоянного развития кибер-угроз специалистам по безопасности всех типов (от CISO до MSP и других провайдеров) необходимо выйти за рамки реактивных подходов к обеспечению ИБ и придерживаться более дальновидной стратегии.

Сама по себе традиционная защита конечных устройств с одним уровнем технологии между Вами и остальным миром уже не жизнеспособна. Учитывая постоянно растущие затраты на квалифицированных специалистов по информационной безопасности, сегодняшние угрозы слишком разнообразны, и они множатся настолько быстро, что ИТ-провайдеры и малые и средние предприятия (SMB) уже не могут зависеть только от ручного управления этими инструментами.

В 2020 году защиты конечных устройств от известных угроз будет уже недостаточно. ИТ-окружения должны быть защищены и от неизвестных угроз тоже, потому что они пытаются оставаться в тени. Для этого ИТ-провайдеры должны пересмотреть свои стратегии ИБ. Новые угрозы требуют перехода от однотехнологичной ИБ к многоуровневым решениям, использующим (помимо других функций) поведенческий мониторинг для устранения постоянных угроз повышенной сложности (APT), безфайловых атак и другой вредоносной активности.

Кроме того, сетевые конечные устройства всех типов, от рабочих станций до ноутбуков и серверов, требуют такого подхода, который объединяет вместе передовую защиту конечных устройств (EPP) и возможности обнаружения и реагирования на атаки против них (EDR) с системой безопасности по принципу "нулевого доверия" (zero-trust), поддерживаемой искусственным интеллектом. Это необходимый сдвиг в том, как индустрия ИБ должна решать проблему кибер-угроз: разрешать запуск на конечных устройствах только известных, зарегистрированных и классифицированных невредоносных программ и процессов (goodware), не давая никаких шансов неизвестным и вредоносным процессам. Такие многоуровневые технологии обеспечивают беспрецедентный уровень контроля, видимости и гибкости, необходимый в динамичной войне с неизвестными злоумышленниками и угрозами.

Данные, собранные антивирусной лабораторией PandaLabs компании Panda Security, осветили несколько новых тенденций в сфере кибер-угроз, которые требуют передовых комплексных решений ИБ следующего поколения для борьбы с ними.

В связи с этим мы создали данный отчет "Понимание угроз 2020", чтобы помочь Вам в защите от новых угроз. Правильная комбинация средств защиты - это не только вопрос выбора того или иного решения ИБ, сколько ответ на серьезный вызов: защититься от завтрашних угроз или стать их добычей.

| Ключевые аспекты

Шифровальщики по-прежнему опасны и вездесущи: один неверный клик может причинить ущерб всей сети.

Все большую обеспокоенность вызывают безфайловые атаки, т.к. их сложнее обнаруживать и они предоставляют скрытные возможности для повреждения всей сети.

Проактивная охота за угрозами (threat hunting) теперь является важным решением для распознавания вредоносного поведения наряду с использованием только надежных и проверенных приложений.

Решения ИБ не могут больше основываться на одной технологии: многоуровневый технологический подход в сочетании с подходом по принципу "нулевого доверия" (zero-trust) обеспечивают отсутствие брешей в надежной системе безопасности.

Введение

Кибер-угрозы растут и развиваются. Пока Вы читаете этот отчет, разрабатываются новые атаки, использующие эксплойты, которые построены на известных уязвимостях, найденных в операционных системах, приложениях и даже человеческом поведении.

В целом, кибер-преступники преследуют три цели:

Финансовая выгода, благодаря шифровальщикам для вымогательства денег.

Данные, которые могут быть проданы в "теневом Интернете".

Контроль над инфраструктурой, сетями и другими важными системами - этот доступ можно продать таким влиятельным игрокам, как государственные спецслужбы, политические группы, преступные группировки и др.

Для SMB, местных органов власти и критически важных организаций опасность кибер-угроз стала неизбежной. Всего за несколько лет менталитет изменился от "это не случится со мной" до "это только вопрос времени". Теперь - это неоспоримый факт: существует неотъемлемый риск для работы компьютерной сети, а инцидент безопасности может нанести непоправимый ущерб организации.

К счастью, по мере развития кибер-угроз также развиваются технологии ИБ. Давно прошли времена простых и медленных антивирусов, работающих "постфактум". Современные решения ИБ используют целый ряд технологий, предназначенных для защиты сетей от проникновения, остановки вредоносного поведения и сдерживания будущих вторжений. Но не все решения ИБ одинаковы. Некоторые построены на старой архитектуре и не могут адаптироваться к новым угрозам. Другие основаны на сигнатурном обнаружении угроз. А какие-то из них пока не совершенны, оставляя слишком большое количество угроз незамеченными.

В то время, когда рынок ИБ наводнен стремлением предоставить для CISO, MSP, ИТ-провайдеров и SMB единственное решение, идеальное для всех, то как можно отсеять этот "шум" и выбрать наиболее подходящий вариант?

Как и в большинстве случаев, все начинается с правильных вопросов.

Зачем реагировать на кибер-угрозы?

Что есть еще, что не видит решение? Ждать ли мне в будущем атаки с их стороны?

Почему решению ИБ следует обнаруживать только те угрозы, которые "работали" (например, проникали в сеть)?

Очевидно, что методы реактивной ("постфактум") безопасности более не жизнеспособны. В любой ИТ-среде существует слишком много угроз и векторов атак, которые несут риски целостности защиты. Современные решения ИБ должны работать на опережение, быть проактивными и готовыми ко всему, что может произойти: они должны быть и щитом, и мечом.

Это привело к созданию многоуровневой технологической модели в сочетании с подходом безопасности по принципу "нулевого доверия", которая не позволяет выполнять на конечных устройствах в сети любые неизвестные процессы.

Результаты анализа в данном отчете покажут, почему решения следующего поколения для защиты конечных устройств успешно используют такой подход, и почему он не только логичен, но и обязателен.

Методология

Данный отчет основан на телеметрии и данных по обнаружению угроз, которые мы получили в 2019 году от локальных агентов семейства решений Panda Adaptive Defense, установленных на конечных устройствах. Полученные данные были проанализированы специалистами лаборатории PandaLabs и Центром операций безопасности компании Panda Security. Наша лаборатория PandaLabs выступает в качестве центра всей нервной системы, реагирующей на угрозы, и помогает формировать технологии Panda.

PandaLabs поддерживает постоянную бдительность, внимательно отслеживая различные тенденции и события в сфере кибер-угроз и атак, чтобы формулировать прогнозы, тактики и стратегии для будущих угроз, и предупреждать общественность о неминуемой опасности.

Специалисты по информационной безопасности в лаборатории PandaLabs обеспечивают непрерывность контрмер в режиме реального времени, позволяя защищать клиентов Panda Security от всех типов угроз в глобальном масштабе. Они также углубляются в экспертный анализ вредоносных активностей, выполняя детальные анализы всех типов угроз для совершенствования решений защиты и информирования общественности.

Уникальные телеметрические данные

Технологии Adaptive Defense осуществляют непрерывный мониторинг всех действий, вызванных запущенными процессами на защищаемых конечных устройствах. Каждое событие каталогизируется на основе более чем 2000 уникальных характеристик объекта. Эти события телеметрии не рассматриваются в качестве инцидентов, вредоносных объектов или аномалий: вместо этого они представляют собой информацию, связанную с определенным объектом, например:

Процессы: создание процесса, его выполнение, внедрение в другое (дочернее) событие и т.д.

Файл: создание нового файла событием/процессом, изменение, удаление, открытие файла и другие операции.

Коммуникации: открытие сокета, использование протокола, направление, источник коммуникации и пр.

Реестр: создание, редактирование или удаление ключей реестра.

Администрирование: использование администраторских учетных данных, события авторизации/выхода, установка процессов, активность сервиса, и многое другое.

Эти действия направляются в облачную платформу Panda Security, где они анализируются с помощью техник машинного обучения для автоматического получения расширенных сведений о безопасности. Данная информация позволяет Panda Security классифицировать каждый запускаемый процесс с практически нулевым уровнем ложно-положительных и ложно-отрицательных срабатываний.

Поскольку Panda придерживается подхода "нулевого доверия", то Adaptive Defense отталкивает почти все угрозы, основанные на вредоносных программах, и если какая-либо из них все же сумеет проникнуть на конечное устройство обманным путем или в результате ошибки пользователя, ее запуск будет запрещен. Это достигается благодаря сервису Panda 100% классификации, который предотвращает выполнение неизвестных и неклассифицированных процессов, а также нашим сервисам Threat Hunting, поддерживаемым искусственным интеллектом, которые отслеживают поведение приложений для защиты от безфайловых атак и других сложных, неизвестных угроз.

Таким образом, данные, которые Вы увидите в этом отчете "Понимание угроз 2020", могут отличаться от других подобных отчетов. Впрочем, в этом нет ничего удивительного. Будучи лидером в сфере ИБ с 30-летним опытом работы и уникальными разработками, ставшими эталоном в нашей отрасли, Panda смотрит на то, что будет дальше, т.к. мы сосредоточены на защите конечных устройств от любых угроз любого рода.

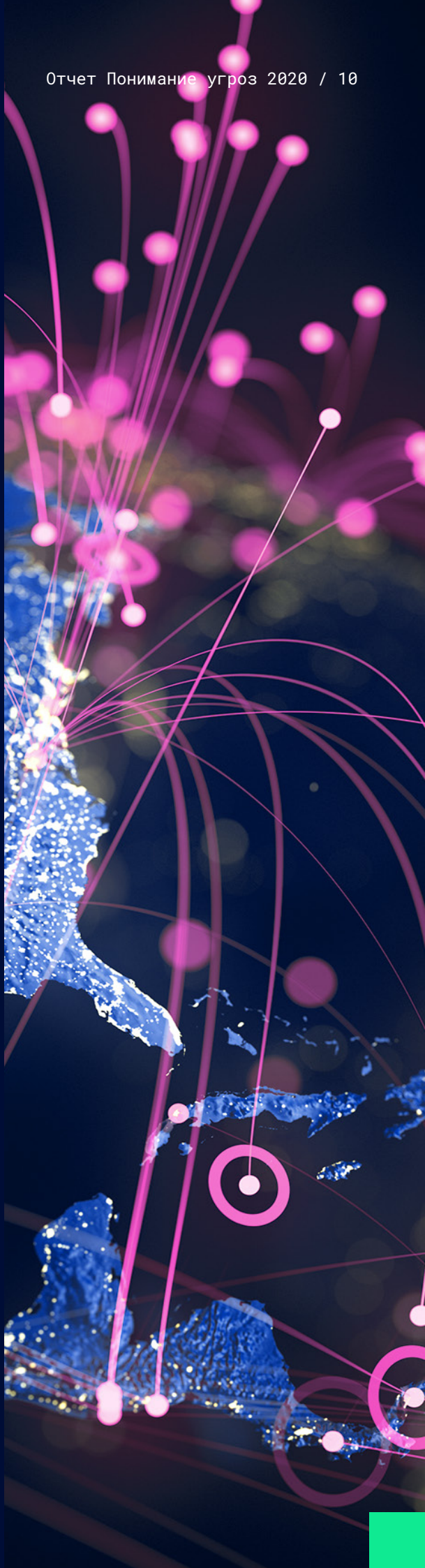
| Результаты

Никаких магических шаров: Данные формируют глобальные знания об угрозах

Безопасность следующего поколения для конечных устройств требует сбора и анализа ошеломляющего объема данных, которые "питают" буквально все: от искусственного интеллекта, осуществляющего контекстный поведенческий анализ и прогноз, до комплексных сервисов Threat Hunting, которые перехватывают угрозы прежде, чем они нанесут свой удар.

Если знания указывают на путь, то в сфере информационной безопасности данные с конечных устройств обеспечивают видимость, которая является неотъемлемой частью в предоставлении лучшего в своем классе решения и необходима для администраторов, ежедневно управляющих своими сетями.

Данные, представленные в этом отчете, показывают не только огромный объем информации, обрабатываемый для достижения оптимальных результатов безопасности конечных устройств с помощью решений следующего поколения, но и важность этих данных для мониторинга всего происходящего на каждом конечном устройстве для обнаружения изменений, трендов и аномалий в глобальном ландшафте угроз. Без такого высокого уровня видимости сегодня и в будущем кибер-преступники, несомненно, смогут достаточно легко "дрейфовать" по сетям.



Понимание на основе данных - это не угадывание

Телеметрические данные Panda, 2019. Значения нормированы на миллион конечных устройств.

Все данные телеметрии, собранные за 2019 год
1,2 петабайт

Обнаружения вредоносного ПО
14,9 млн уведомлений о вредоносном ПО

Выявления исполняемых файлов
426 млн исполняемых файлов идентифицировано

Выполнения приложений
79,5 млн дочерних процессов выполнено (созданные процессы или загруженные библиотеки)

Выявления файлов динамических библиотек (dll)
336 млн файлов выявлено

Примечание: Действия, выполняемые процессами в целом, и эволюция обнаружений вредоносного ПО в сети (не важно, были ли запущены актуальные вредоносные файлы или нет) помогают администраторам принимать решения по определению мер, позволяющих смягчать последствия и корректировать политики безопасности.

Обнаружение и реагирование

Вредоносное ПО
14,9 млн событий

Эксплойты
76 000 уведомлений

Потенциально нежелательные программы (ПНП)
7,9 млн уведомлений

Коммуникации

Сетевые события
1,4 трлн событий

Изменения DNS
2 млрд событий (неудачные DNS-запросы)

Скачивания
1,6 млрд событий

Примечание: Мониторинг сетевых соединений, установленных процессами, - это ключевой фактор при выявлении подозрительных или потенциально опасных направлений, используемых для запуска кибер-атак или кражи данных.

Поведение объекта (файла)

Процессы
1,7 трлн событий

Операции с реестром
735 млн событий

Скрипты
1,9 млрд событий

Выполненных приложений
92 млрд событий

Операций с устройством
973 млн событий

Авторизация/выход
133 млрд событий

Примечание: Подробная информация о поведении объектов позволяет администраторам обратить свое внимание на подозрительные активности, выполняемые новыми, еще не идентифицированными объектами (элементами), и получить данные, которые могут быть использованы для получения выводов об их потенциальном уровне риска.

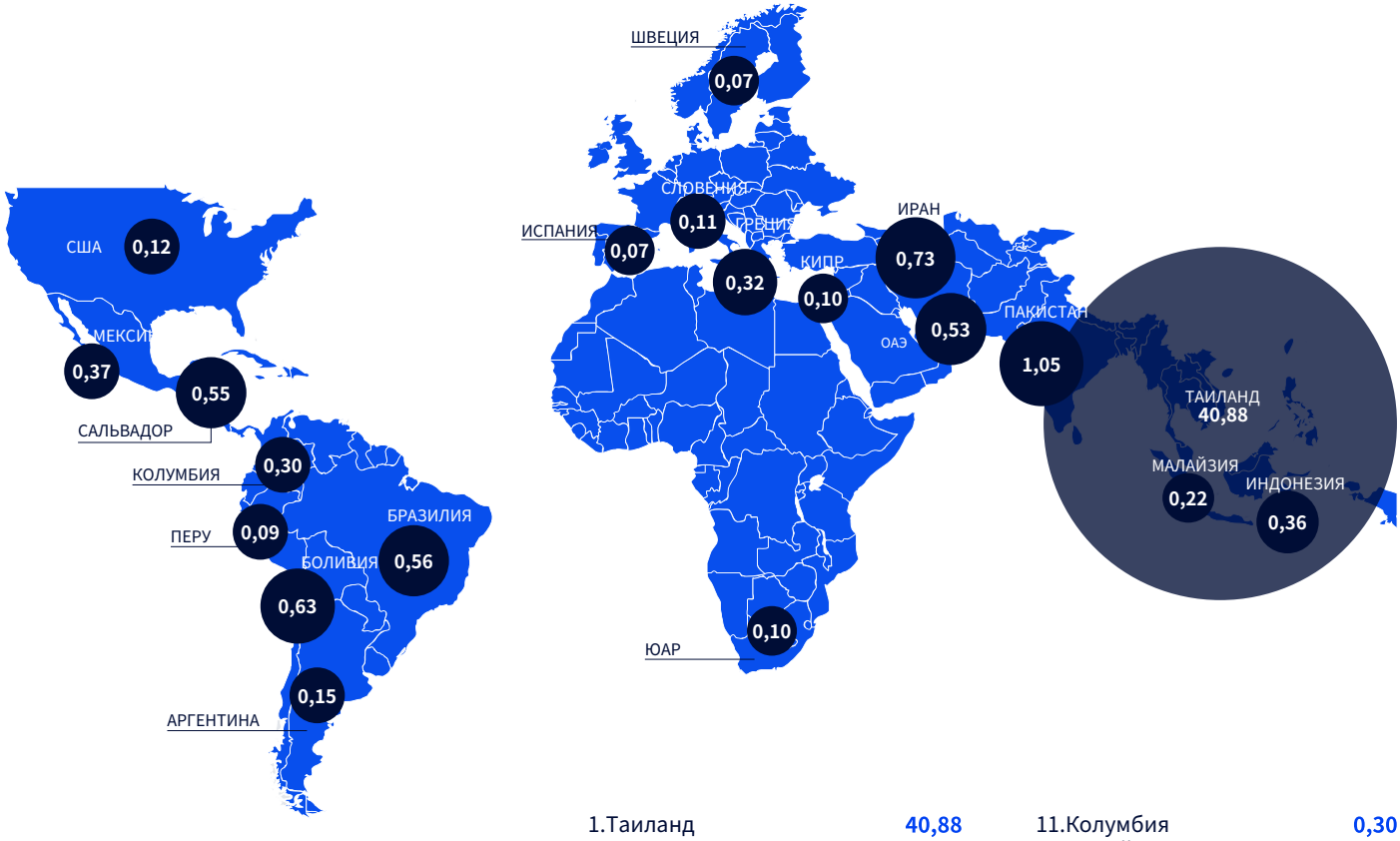
Глобальные хотспоты: Атакующие или атакуемые?

Судя по данным, существует значительный перекос в целях на Ближнем Востоке и в Южной Америке. Впрочем, Таиланд лидирует с серьезным отрывом. Такие результаты могут быть вполне ожидаемыми: эти страны являются хорошими мишенями по той причине, что хакеры в них добились серьезного успеха в компрометации систем в силу недостаточности защиты конечных устройств.

И наоборот, эти атаки были отбиты технологиями Panda, которые показали "пульс" ситуации, характерный для атак в соответствующем регионе. Можно предположить, что эти цели не являются конечными: вероятнее всего, они становятся источниками других, более сложных атак на цели во всем мире.

Топ-20 стран по вредоносным атакам

Рейтинг стран с не менее чем 1000 отчетных устройств, основанный на соотношении числа вредоносных оповещений (не заражений) к количеству отчетных устройств.



1.Таиланд	40,88	11.Колумбия	0,30
2.Пакистан	1,05	12.Малайзия	0,22
3.Иран	0,73	13.Аргентина	0,15
4.Боливия	0,63	14.США	0,12
5.Бразилия	0,56	15.Словения	0,11
6.Сальвадор	0,55	16.Кипр	0,10
7. ОАЭ	0,53	17.ЮАР	0,10
8.Мексика	0,37	18.Перу	0,09
9.Индонезия	0,36	19.Швеция	0,07
10.Греция	0,32	20.Испания	0,07

События доступа к PDF-файлам

Эти данные, собранные с конечных устройств технологиями Panda Adaptive Defense, раскрывают всю "мощь" определенных расширений файлов - многие из них пользователи видят каждый день. И за каждым из этих расширений кроется уязвимость в самой природе таких файлов, которая может использоваться злоумышленниками для осуществления атак.

Вездесущий PDF, используемый каждый день, во главе рейтинга, и не без оснований: на протяжении многих лет этот формат печально известен своей способностью выполнять вредоносные атаки и внедрять вредоносный код в процессы приложения или использоваться для фишинговых кампаний, когда один безобидный клик ничего не подозревающего пользователя приводит к инциденту.

Рейтинг файловых расширений с точки зрения событий доступа к данным

Рейтинг расширений файлов с данными, к которым обращались в 2019 году, и количество зарегистрированных уникальных событий доступа.

№	События	Расширения	Описание
1	220 124 750	.pdf	Файл Portable Document Format
2	178 096 618	.odf	Файл OpenDocument (связан с приложениями MS Office)
3	60 203 323	.job	Объект задачи планировщика задач Windows
4	51 313 631	.pem	Сертификат Privacy Enhanced Mail (для безопасной аутентификации сайта)
5	48 607 743	.mdb	База данных Microsoft Access
6	28 006 668	.xls	Таблица Microsoft Excel (формат 97–2003)
7	25 388 869	.doc	Документ Microsoft Word (формат 97–2003)
8	17 199 902	.cer	Сертификат безопасности Интернета (для проверки подлинности сайта)
9	16 896 788	.pst	Файл хранилища персональной информации MS Outlook (почтовый ящик)
10	10 927 605	.p12	Файл обмена персональной информацией (содержит цифровой сертификат)
11	10 576 428	.dwg	Файл базы данных чертежей AutoCAD
12	9 234 914	.odt	Формат текстового документа OpenDocument
13	8 403 811	.ods	Формат таблицы OpenDocument
14	6 175 198	.ini	Файл инициализации Windows (для загрузки параметров приложения)
15	5 375 405	.ppt	Презентация MS PowerPoint
16	5 100 168	.dat	Общий формат файла данных (генерируется определенными приложениями)
17	4 418 416	.txt	Обычный текстовый файл

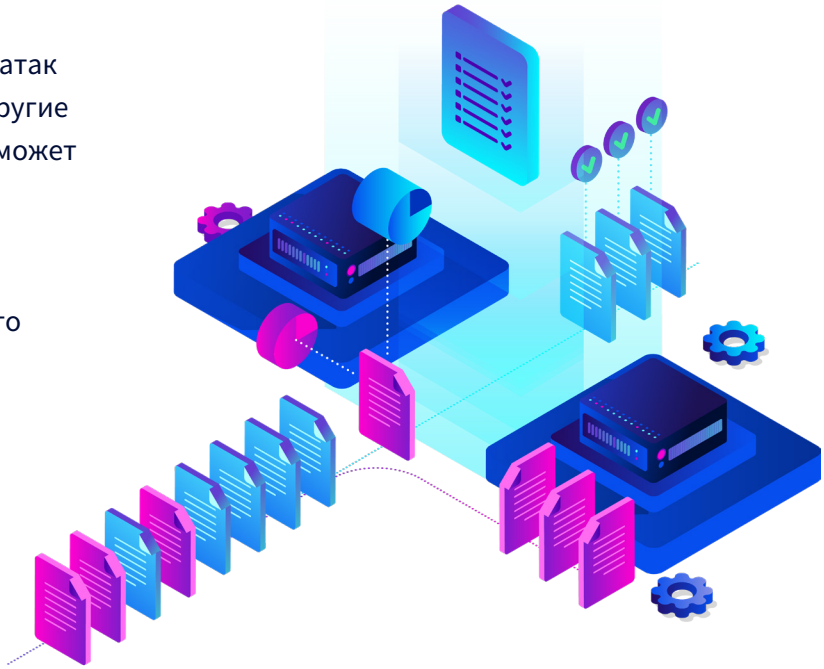
Ограничения белых списков

Черные списки практически также стары, как и сама антивирусная технология, и пока они, безусловно, блокируют множество простых угроз, ограничения "блэклистинга" хорошо известны и они легко обходятся. В наши дни, с развитием подхода безопасности по принципу "нулевого доверия", многие специалисты ИБ видят определенный комфорт в белых списках, в которых содержатся приложения, о которых им хотя бы не приходится беспокоиться. Таким образом, многие решения просто пропускают занесенные в белый список приложения (даже строят свою методологию вокруг этого), полагаясь на то, что они не имеют вредоносного поведения и не выполняют вредоносные процессы.

Но это слабое утешение: белые списки, подобно черным спискам, имеют свои ограничения, и современные угрозы могут не только обходить решения на базе белых списков, но даже использовать их в своих целях. Рост числа безфайловых атак сделал мониторинг невредоносных программ (goodware) еще более важным, т.к. они используют известные и надежные приложения для осуществления атак и незаметного распространения угроз на другие устройства. А поскольку одно приложение может вызывать множество событий, необходимо осуществлять мониторинг поведения и выполнения всех приложений и процессов, выискивая во время охоты на угрозы все, что может выглядеть нелегитимным или подозрительным.

К счастью, есть решение, которое выходит за рамки белых списков, и это - активный мониторинг всех приложений и процессов. Когда полностью отслеживается вся активность на конечных устройствах, вредоносные программы всегда будут выявлены и запрещены к запуску, а невредоносные программы (goodware) не будут использоваться для незаконных целей.

Каждый раз, когда на конечных устройствах, защищенных решением Panda Adaptive Defense, пытается запуститься приложение или загружается библиотека, защита проверяет, является ли оно надежным, с помощью локальной и облачной репутационной системы или общей сигнатуры сперва в локальном кэше, потом в облачной базе знаний (она также передает данные в локальный кэш для будущих запросов). Облачная база знаний постоянно получает сведения от сервиса классификации (машинное обучение и аналитики PandaLabs) в виде хэшей файлов и их классификации в виде goodware, malware или ПНП.

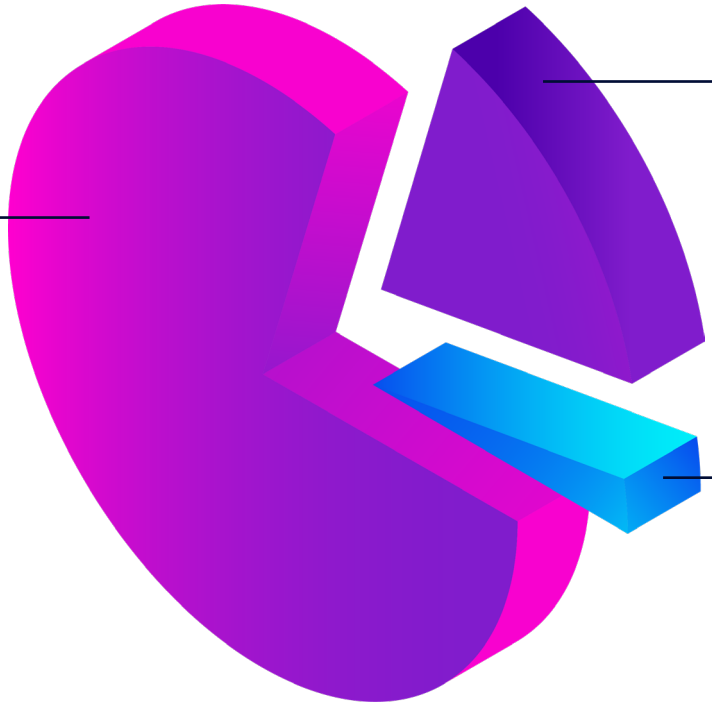


В то же время машинное обучение непрерывно обрабатывает новые данные, получаемые от процессов, запускаемых на миллионах защищаемых конечных устройств. Поскольку неизвестные файлы могут быть заблокированы до тех пор, пока не станет известна их классификация, они также запускаются на "ферме" физических (не виртуальных) конечных устройств, расположенных в облаке. Это позволяет системе машинного обучения извлекать знания из наблюдения за их реальным поведением со временем. Эти новые знания оцениваются для того, чтобы классифицировать их с максимальной достоверностью и в кратчайшие сроки.

Активность конечных устройств также непрерывно отслеживается в реальном времени при выполнении всех невредоносных программ (goodware) и их контекста (события, происходящие во время их выполнения, пользователи, выполняющие каждую команду или приложения, генерируемый сетевой трафик, доступ к файлам с данными, события до и после операций и пр.). Все эти данные помогают выявить высоконадежные индикаторы атак (IoA) без ложных срабатываний.

Мониторинг и выполнение приложений

Отдельные приложения, запущенные на защищаемых конечных устройствах на помесячной основе на каждый миллион устройств в 2019 году (примерные данные).



Выполнено приложений: **5 миллионов**

18% приложений, идентифицированных в PandaLabs, были новыми

0,6%–1,2% были классифицированы как полностью неизвестное вредоносное ПО, которые ускользали от любого другого уровня технологии

Новая угроза: Безфайловые атаки

Эти данные подтверждают глобальные позиции "живого" хакинга при использовании эксплойтов и инструментов повышения производительности, браузеров и компонентов ОС, которые присутствуют на большинстве устройств во всем мире и обычно занесены в белые списки. Ни одно приложение или исполняемый файл в этом списке не будут классифицироваться как подозрительные, позволяя угрозам делать их идеальными векторами для безфайловых атак, "живому" хакингу, LotL-атакам...

Этот список показывает абсолютную необходимость в технологии защиты от эксплойтов. Учтите, что нет единого общего знаменателя в отношении того, почему каждое из этих приложений выбрано хакерами. Например, Microsoft IIS используется за свою способность обращаться к многочисленным сайтам, а макросы Microsoft Office открывают возможность логировать экран и клавиатуру, поэтому для обнаружения таких атак необходим контекстный поведенческий анализ.

Топ-10 эксплуатируемых приложений

Приложения, в которых технологии Adaptive Defense обнаружили наибольшее число атак через эксплойты.

#	Название	Исполняемый файл	Кол-во новых уязвимостей в 2019 году (CVE)	Вендор	Тип приложения
1	**Firefox**	firefox.exe	**105**	Mozilla	Интернет-браузер
2	**Microsoft Outlook**	outlook.exe	**7**	Microsoft	Почтовый клиент
3	**Internet Explorer**	iexplore.exe	**53**	Microsoft	Интернет-браузер
4	**Microsoft Word**	winword.exe	**5**	Microsoft	Текстовый редактор
5	**Internet Information Services (IIS) Manager**	w3wp.exe	**Н/Д**	Microsoft	Веб-сервер
6	**Microsoft Excel**	excel.exe	**7**	Microsoft	Таблицы
7	**Adobe Reader**	acroRd32.exe	**Н/Д**	Adobe Systems	PDF-ридер
8	**Winamp**	winamp.exe	**Н/Д**	Nullsoft	Медиа-проигрыватель
9	**Microsoft Access**	msaccess.exe	**Н/Д**	Microsoft	СУБД
10	**Google Chrome**	chrome.exe	**177**	Google	Интернет-браузер

Примечание: Н/Д означает отсутствие новых задокументированных уязвимостей в 2019 году. Возможно, использовались более старые или неизвестные уязвимости.
Источник: https://www.cvedetails.com

Одно решение, много уровней

Кибер-угрозы не похожи друг на друга, и там, где технология останавливает одну угрозу, она может пропустить другую. Для обнаружения и реагирования на кибер-угрозы в 2020 году потребуется сочетание локальных сигнатурных технологий, облачных технологий и контекстного поведенческого анализа.

Однако цифры не говорят всей правды. Хотя технология с локальными сигнатурами может обнаруживать многие угрозы (отчасти это связано с тем, что многие атаки известны, а использовать сигнатуры экономически эффективно), но все же они не могут останавливать те угрозы, которые находит контекстный поведенческий анализ, потому что они, как правило, более сложные и потенциально более опасные. Таким образом, в 2020 году применение нескольких уровней для борьбы с всем спектром угроз является оптимальным подходом, обеспечивающим максимально эффективное предотвращение всех угроз.

Почему так важна многоуровневая безопасность

Посмотрите, где останавливаются угрозы и почему важно использовать многоуровневые технологии информационной безопасности. Данные взяты за 30 дней с конечных устройств, защищенных решением Panda Adaptive Defense.

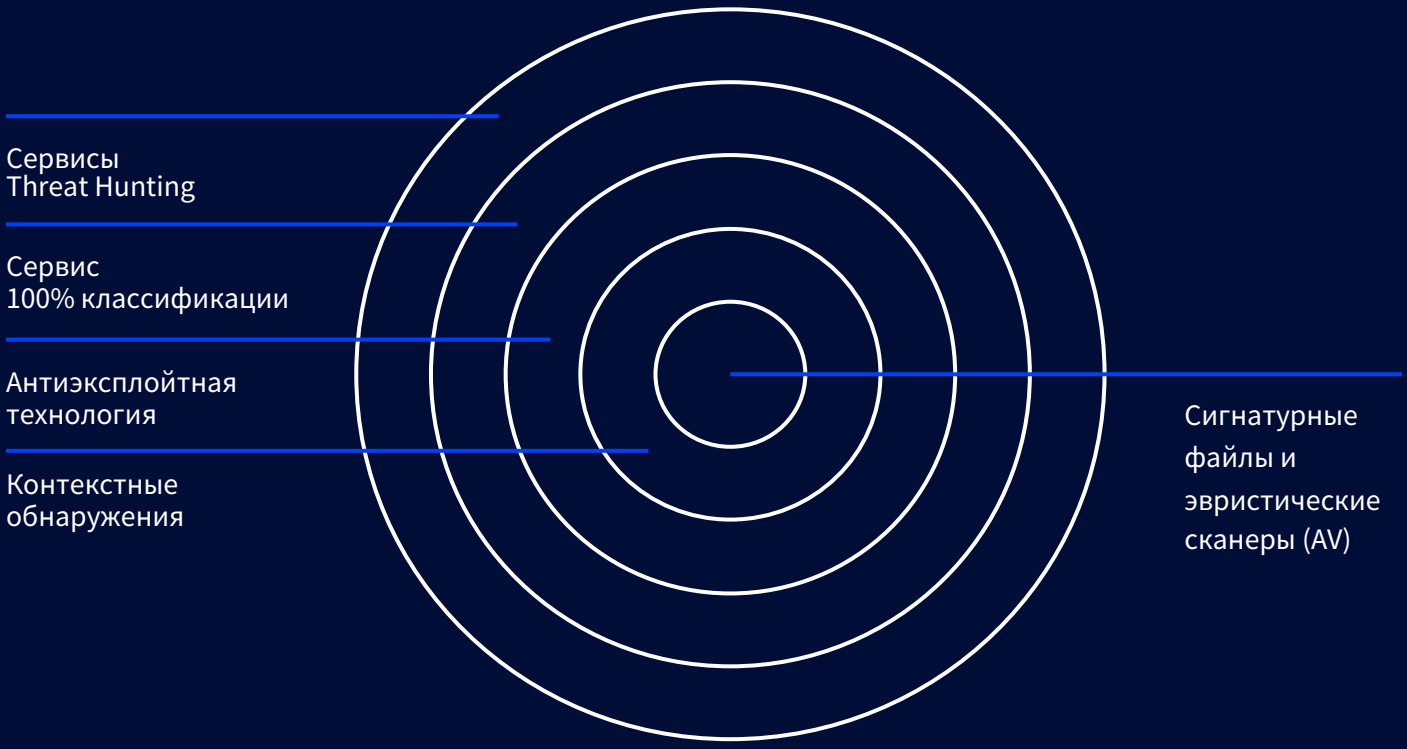
		Технология обнаружения	Описание
Конечных устройств	47 648	Локальные сигнатуры	Проверяет наличие хэшей файлов в кэше известных вредоносных объектов, хранящемся локально на конечном устройстве.
Обнаружено инцидентов	598 952		
Конечных устройств	49 228	Облачное обнаружение	Проверяет облачную базу знаний в реальном времени на наличие вредоносного объекта и отправляет данные в локальный кэш для будущих запросов. Облачная база знаний непрерывно пополняется данными от сервиса 100% классификации.
Обнаружено инцидентов	500 534		
Конечных устройств	7 828	Контекстный поведенческий анализ	Анализ контекста выполнения для выявления индикаторов атаки на конечное устройство. Запрещает выполнение дочерних процессов и может блокировать/удалить родительские процессы. Данная технология также позволяет блокировать атаки, использующие инструменты/скрипты администрирования, и обнаруживать атаки в памяти, например, обнаружение внедрения в память кода, не отображенного в файле, хранящемся на диске.
Обнаружено инцидентов	250 733		

Заключение

Кибер-угрозы никогда не были столь разнообразны, как в 2020 году. В любой день конечное устройство может столкнуться с фишинговой аферой со ссылкой на вредоносный файл, заполучить шифровальщик с поддельного веб-сайта, пасть жертвой коварной безфайловой атаки, которая способна скрываться в памяти неделями, месяцами или даже дольше.

В то время, когда число угроз постоянно растет, а сами угрозы эволюционируют, ИТ-специалисты должны внедрять все доступные для них инструменты, чтобы обеспечивать безопасность своих сетей.

Panda Adaptive Defense:
Решение, признанное рынком и аналитиками, для предотвращения существующих и перспективных угроз



Panda Adaptive Defense состоит из нескольких уровней технологии ИБ, работающих одновременно для защиты от кибер-атак и их последствий. Эти уровни могут быть сгруппированы в виде технологий защиты конечных устройств **Endpoint Protection (EPP)** и технологий обнаружения атак на конечные устройства и реагирования на них **Endpoint Detection and Response (EDR)**.

panda

Уровни технологии защиты конечных устройств

Сигнатурные файлы и эвристические сканеры

Широко известный как традиционная антивирусная технология (AV), данный уровень доказал свою эффективность против многих распространенных угроз низкого уровня. Это оптимизированная технология для обнаружения известных атак, основанная на сигнатурах, общем и эвристическом обнаружении и блокировке вредоносных URL.

+ 10 000
событий
каждый день

Поведенческий анализ

Используется для обнаружения аномального поведения ресурсов и приложений: данный уровень необходим для обнаружения безфайловых атак и атак без использования вредоносного ПО. Эффективен, среди прочего, против атак на основе скриптов и с использованием легитимного ПО (например, PowerShell, WMI и т.д.), уязвимостей в браузерах и других часто атакуемых приложениях (Java, Adobe Reader, Adobe Flash, Microsoft Office...). Технология контекстного обнаружения Panda постоянно развивается, адаптируясь к новым угрозам, благодаря полной видимости, обеспечиваемой для Panda Adaptive Defense.

3 триллиона
событий в
Data Lake

Антиэксплойтная технология

Эта технология призвана обнаруживать безфайловые атаки, которые предназначены для обнаружения уязвимостей. Дополняя технологию контекстного обнаружения Panda, она ищет и обнаруживает аномальное поведение - верный сигнал эксплуатируемых процессов. Технология важна для всех конечных устройств, но критически важна для тех устройств, которые не пропатчены (или ожидают применения патчей), или на которых установлена не поддерживаемая более ОС.

2 миллиона
новых бинарных
файлов,
классифицируемых
каждую неделю

panda

Уровни технологии защиты конечных устройств

Сервис 100% классификации

Традиционные EDR-решения идентифицируют вредоносные программы, но ничего более, что может создавать риск. Благодаря нашему сервису 100% классификации, решение Panda Adaptive Defense осуществляет мониторинг не только всех приложений как таковых, но и все запущенные процессы в системе. Благодаря этой "зрелой" технологии EDR (более пяти лет эксплуатации), отпадает фактор неизвестности по отношению к исследуемым объектам: решение разрешает только те процессы, которые известны в лаборатории Panda и классифицированы как "надежные" процессы. Этот уникальный управляемый сервис - ключевой компонент Panda Adaptive Defense, обеспечивающий максимальную защиту устройств без необходимости делегирования конечным пользователям принятия важных решений ИБ. Кроме того, данный сервис обеспечивает высокий уровень защиты в случае, если предыдущий уровень не смог остановить атаку на уже инфицированных компьютерах и горизонтальные перемещения атаки внутри сети. Его подход, основанный на искусственном интеллекте, обеспечивает автоматическую классификацию 99,98% приложений, а оставшиеся 0,02% приложений проверяются и классифицируются экспертами PandaLabs. Это единственная технология такого рода, доступная на рынке в наши дни.

Threat Hunting & Investigation Service

Единственный в своем роде стандарт, который может быть включен в EDR-решение, сервис Panda Threat Hunting & Investigation Service (THIS) для "охоты за угрозами" и их исследования - это проактивный сервис, который обнаруживает скомпрометированные машины, атаки на самых ранних этапах и подозрительную активность. Когда все остальные технологии терпят неудачу против чрезвычайно сложных атак, порой месяцами остающихся незамеченными, Threat Hunting может искоренить их при использовании набора упреждающих процедур. Управляемый экспертами глобальной команды Panda по информационной безопасности, сервис THIS способен находить даже малейшие следы, оставленные хакерами в своих попытках заполучить контроль над конечным устройством с помощью техник living-off-the-land (LOTL).

Будущее информационной безопасности лежит не в едином методе защиты, а в сочетании эффективных и проверенных уровней технологии безопасности с передовыми решениями, способными прогнозировать развитие ситуации. Такой подход является наиболее эффективным и действенным способом проактивно защищать конечные устройства от известных и неизвестных угроз. И поскольку угрозы в 2020 году стали все более сложными, то конечным пользователям и ИТ-провайдерам всех размеров требуется решение информационной безопасности, которое постоянно идет на шаг впереди хакеров.

Демо-консоль

Связаться с нами

Подробнее:
pandasecurity.com/business

Обсудить:
communication@pandasecurity.com