ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт Центра мониторинга за первое полугодие 2018 года

Отчёт за I квартал 2017 года.

Отчёт за II квартал 2017 года.

Отчёт за второе полугодие 2017 года.

Что и как мы считаем

- **Событие ИБ** — идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
- **Инцидент ИБ** — появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

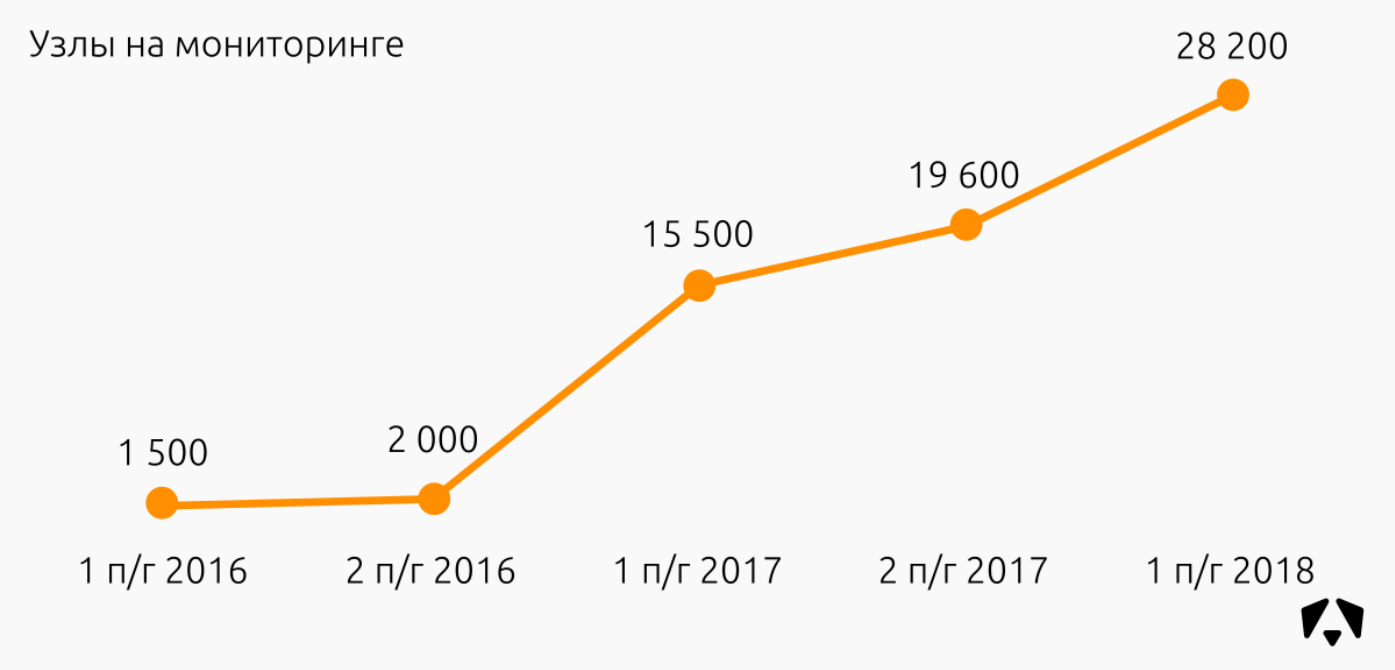
Источниками событий выступают сетевые и хостовые IDS, сетевые устройства, сканеры защищённости, антивирусные решения и honeypot'ы.

В рамках внутренней обработки мы классифицируем инциденты в зависимости от затронутых ресурсов.

Высокая критичность	Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
Средняя критичность	Инциденты, связанные с некритичными ресурсами серверного сегмента.
Низкая критичность	Инциденты, связанные с некритичными ресурсами пользовательского сегмента (рядовой пользователь).

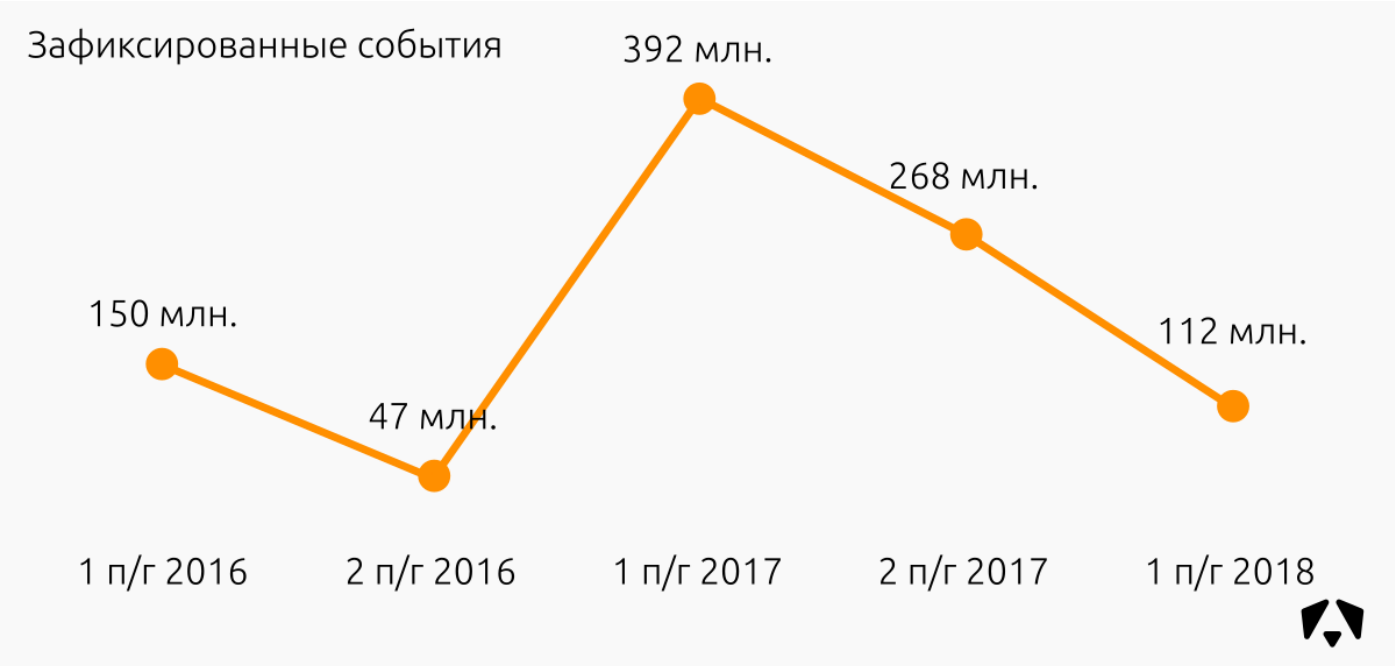
Аналитик Центра мониторинга произвольно определяет степень критичности, если считает, что инцидент может привести к серьёзным негативным последствиям.

Результаты мониторинга



В период **с 1 января по 30 июня 2018 года** сотрудники Центра мониторинга контролировали информационные системы организаций с общим числом подключённых узлов около **28 200** (рабочие места, веб, почта, файловые хранилища и т. д.). Благодаря растущему интересу к тематике создания и эксплуатации центров мониторинга информационной безопасности нам удалось за первое полугодие 2018 года привлечь новых постоянных клиентов и запустить несколько пилотных проектов.

За шесть месяцев 2018 года сенсоры зафиксировали **112 млн. событий** информационной безопасности.



Снижение количества зарегистрированных событий ИБ, с учётом увеличения количества контролируемых ресурсов и инцидентов, обусловлено следующими факторами:

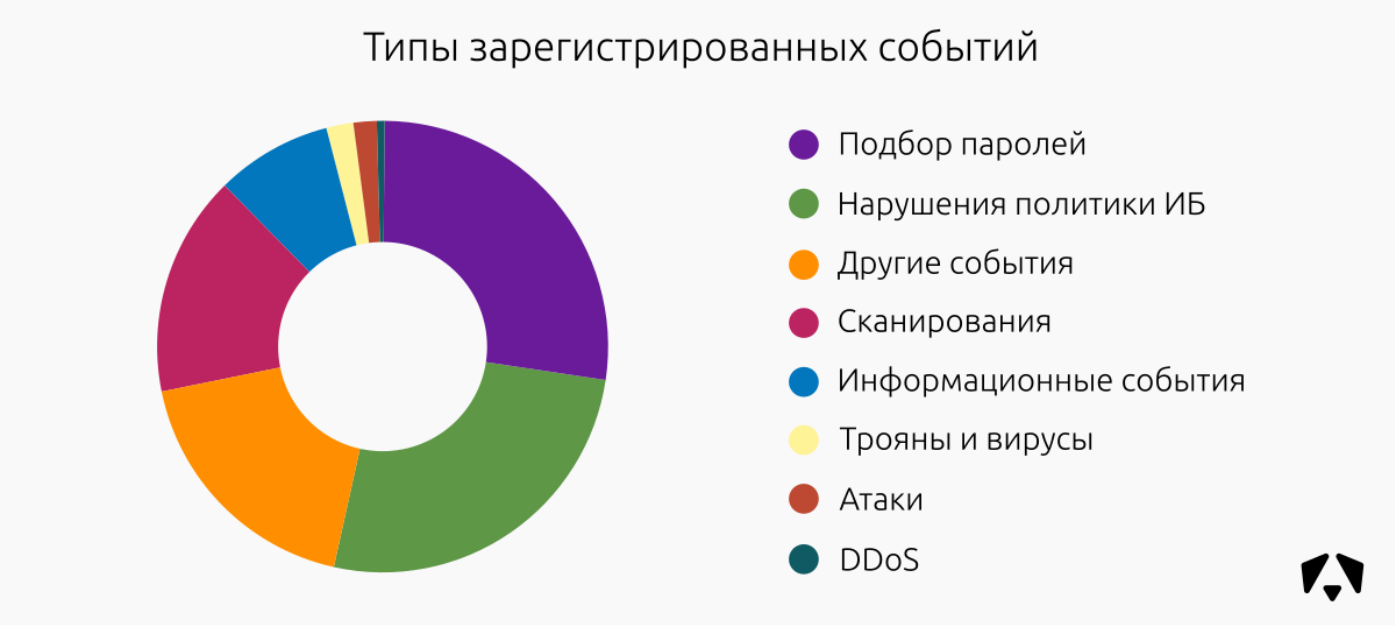
1. Наши сигнатурные аналитики дорабатывают сигнатуры, которые дают большое число false-positive срабатываний в конкретной контролируемой информационной системе. Благодаря

уже значительному опыту в написании правил и оценке их поведения в разных организациях, сигнатуры стали менее зависимыми от особенностей сети и более унифицированными, в то же время, не теряя эффективности при наличии «плохого» трафика.

2. Были оптимизированы некоторые правила базы AM Rules. Благодаря этому множество одинаковых событий агрегируются.
3. Благодаря первым двум пунктам Центр мониторинга быстрее реагирует на DDoS-атаки и другие инциденты ИБ, проявляющиеся в большом количестве срабатываний сигнатур, и помогает предотвращать их развитие на ранней стадии.

Было зарегистрировано **434 инцидента**.

Двадцатипроцентный рост количества инцидентов по сравнению со вторым полугодием 2017 года вызван тем, что к Центру мониторинга активно подключались новые заказчики. А новая инфраструктура на мониторинге — это почти гарантированно всплеск количества выявленных инцидентов, которые владелец инфраструктуры ранее просто не мог заметить. Стоит разобраться с этим «новым пиком», и количество зафиксированных инцидентов резко снижается.



«Информационное событие» — события, несущие информационную направленность, которые могут быть полезны при разборе инцидента.

«Нарушение политики ИБ» — события, свидетельствующие о действиях, предположительно нарушающих требования Политики ИБ контролируемой организации.

«Атака или эксплуатация» — события, свидетельствующие о попытках удалённого исполнения кода или эксплуатации уязвимостей на контролируемых ресурсах.

«Сканирование» — события, свидетельствующие об исследовании сети перед попыткой атаки.

«Подбор паролей» — события, свидетельствующие о попытках получения доступа к контролируемым ресурсам путём подбора аутентификационных данных.

«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«DDoS» — события, свидетельствующие о попытках осуществления распределённых атак на отказ в обслуживании.

Распределение зафиксированных событий по типам не сильно изменилось по сравнению со второй половиной 2017 года. Самое заметное изменение — выход на первое место попыток подбора паролей к различным сервисам. Нарушения политик, сканирования и информационные события всё так же остаются в «топе».

Увеличилось количество событий в категории «Сканирование». В первом полугодии у нас увеличилось число клиентов, а, следовательно, и количество узлов. Если контролируемый узел смотрит напрямую в интернет, то он ежедневно подвергается большому количеству сканов ботами. Большинству клиентов приоритетнее контролировать атаки из внешней сети, поэтому и на мониторинг ставят узлы с белыми адресами. От этого прирост в «Сканированиях» и сокращение «Информационных событий», больше свойственных внутренним узлам.

Зафиксированные инциденты

Среди выявленных **434 инцидентов**:

Класс инцидента	Низкая критичность	Средняя критичность	Высокая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	3	75	101	179	41%
Атаки и попытки эксплуатации уязвимостей	4	68	57	129	30%
Подбор паролей	2	27	35	64	15%
Нарушение политики ИБ	6	32	6	44	10%
DDoS	3	5	10	18	4%
Всего:	18	207	209	434	100%

По самому большому классу — вредоносное ПО, мы наблюдали следующие тенденции:

1. Чем больше узлов на мониторинге — тем больше инцидентов с ВПО.
2. Как и во втором квартале 2017 года продолжаются заражения семейством вредоносов WannaCry и Petya/notPetya. Несмотря на всеобщее освещение этой проблемы, всё равно остаётся очень много уязвимых узлов.
3. Большинство найденных вредоносных файлов представляют собой ПО для майнинга криптовалют. Хакеры стали немного «добрее» и пытаются заработать на ресурсах пользователей.
4. Также часто находим рекламное потенциально-нежелательное ПО. В основном пользователи скачивают его вместе с взломанными или бесплатными программами и при установке ПО для быстрого поиска драйверов, например, DriverPack и аналоги.

Что касается «Эксплуатации уязвимостей», то мы продолжаем наблюдать большое количество попыток эксплуатации уязвимостей в Apache Struts, Drupalgeddon, и EternalBlue.

Большое количество инцидентов заведено на эксплуатацию уязвимости EternalBlue. Звучит печально, но статистика показывает, что пользователи до сих пор не защитились от столь нашумевших уязвимостей. Несмотря на то, что загрузка шифровальщиков через данную уязвимость уже минимальна, её активно используют для распространения другого вредоносного ПО. И если зашифрованные данные видны сразу, то активность другого вредоносного ПО обычный пользователь может даже и не заметить.

Например, в конце июня нами было проведено исследование заражённой шифровальщиком машины. Мы выявили, что деструктивные действия были осуществлены через удалённое подключение к системе. Злоумышленник запустил программу-шифровальщика и спустя несколько минут отключился от узла жертвы.

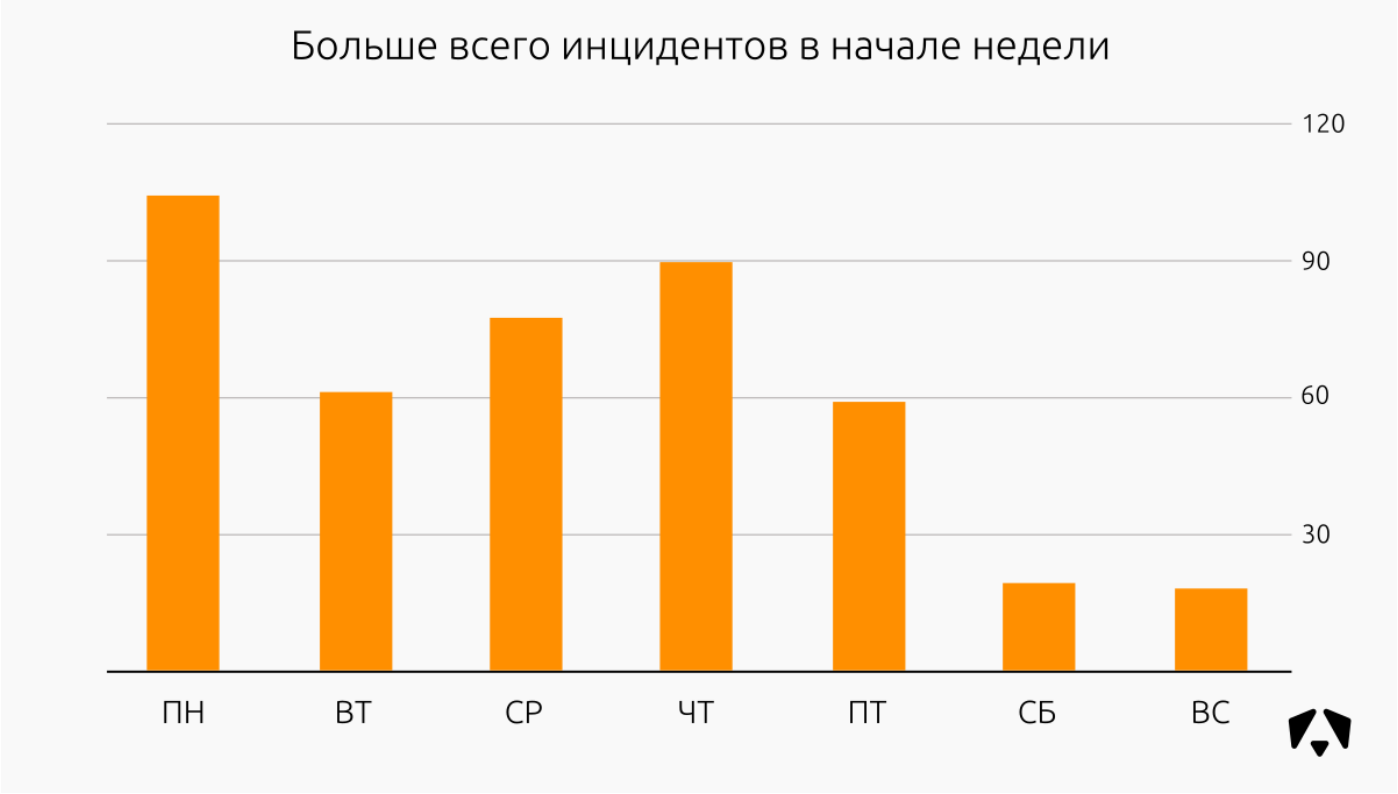
Наши исследователи нашли файл запущенного шифровальщика, замаскированный под процесс svchost.exe (программа-шифровальщик семейства GlobeImposter 2.0, как выяснилось в ходе детального анализа файла), а также следы запуска других подозрительных программ. Среди них была установленная утилита ProcessHacker (с KProcessHacker драйвером). С её помощью злоумышленник завершил привилегированные процессы и освободил занятые процессами файлы для их последующего шифрования. Хакер на этом не остановился и, воспользовавшись случаем, внедрил в заражённую систему майнер (почему бы не взять по максимуму?).

Файлы для майнинга криптовалюты Litecoin (LTC) были обнаружены в системной директории. Среди них был сам файл майнера, библиотеки для поддержания многопоточности и отправки HTTP-запросов, а также программа, которая все это собирала и запускала с нужными злоумышленнику параметрами. Этот файл был добавлен в Планировщик заданий и запускался при каждом старте системы.

Если бы злоумышленник не запустил на взломанной системе шифровальщик, то, возможно, владелец АРМ и не заметил бы стороннего присутствия. А ресурсы системы были бы использованы для добычи криптовалюты и/или атаки на других пользователей в локальной сети.

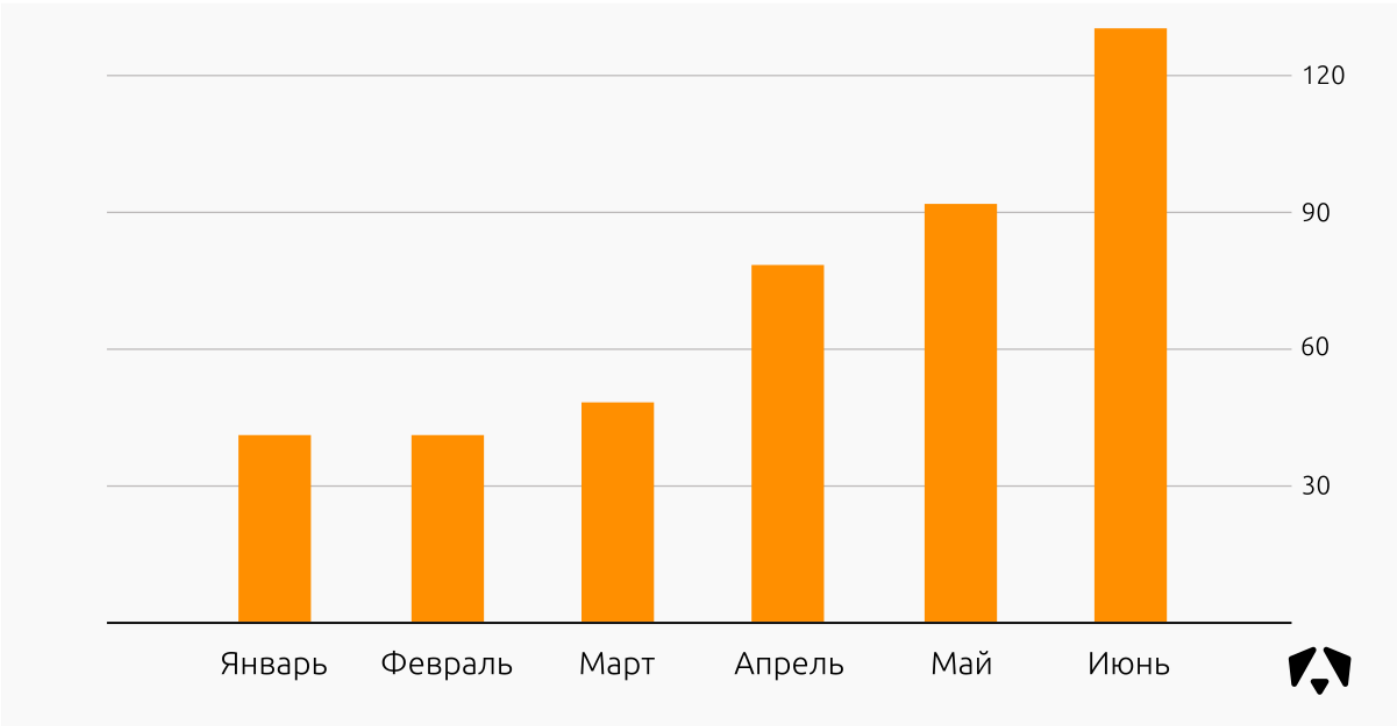
Остальную массу заведённых инцидентов в категории составляют попытки эксплуатации XSS, внедрение PHP- и SQL-инъекций.

Распределение инцидентов ИБ относительно дней недели в первом полугодии 2018 года:



Обычно именно в понедельник проводятся фишинговые рассылки, отправляют вредоносное ПО, замаскированное под сверки, акты и т. д. Скорее всего, такая активность направлена на ещё не отошедших от выходных людей. Также основную массу новых клиентов мы подключаем с начала недели, что тоже даёт большой прирост в событиях, особенно это касается таких категорий как подбор паролей, атаки и эксплуатаций уязвимостей.

Распределение инцидентов ИБ за первое полугодие 2018 года:



Прирост по инцидентам связан с расширением сетей наших клиентов. Как минимум 2 организации к апрелю увеличили количество сенсоров на контролируемых объектах. Плюс к этому весной и летом было много пилотных проектов.

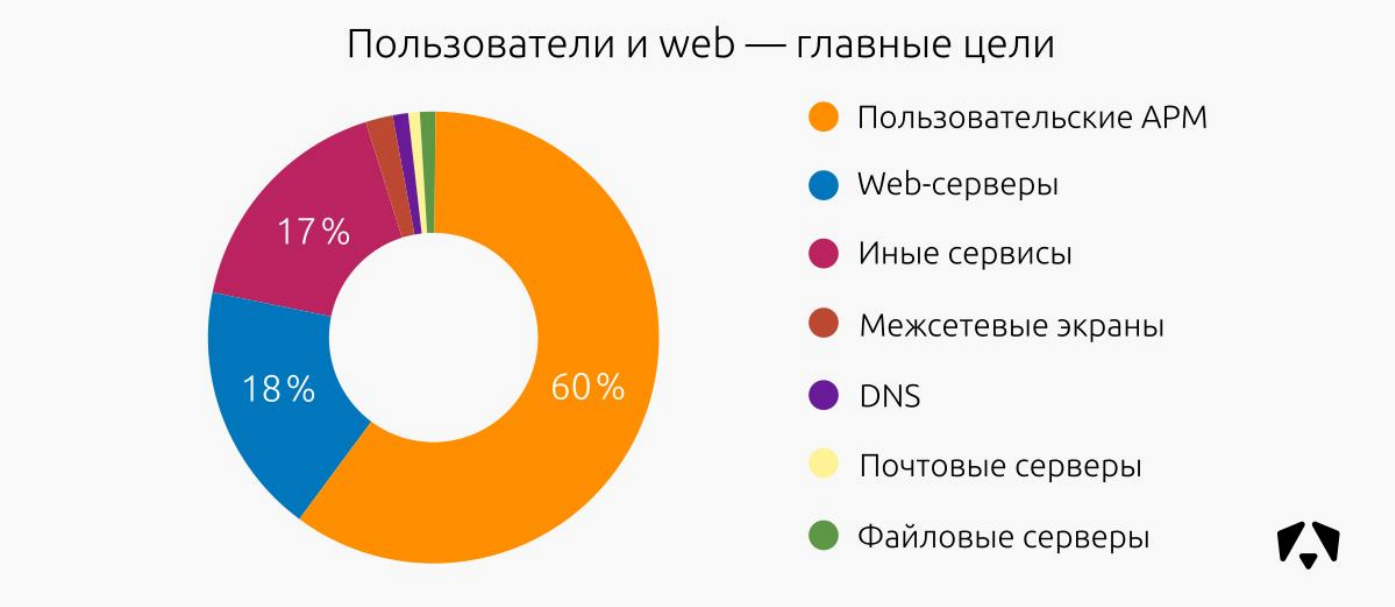
Также наши сигнатурные аналитики постоянно пишут правила на свежие уязвимости, что помогает отлавливать новые атаки на ресурсы клиентов.

ТОП источников

Под источниками атак в данном случае понимаются IP-адреса, которые были участниками сетевого взаимодействия с контролируемыми адресами и пытались нанести вред инфраструктуре.

На карте отражено расположение первой сотни IP-адресов по количеству зарегистрированных событий. Большинство таких адресов расположено в России, Украине, Китае, США, Германии и Нидерландах.

ТОП сегментов, подверженных инцидентам



В первом полугодии 2018 года наиболее часто подвергались нежелательному воздействию именно пользовательские АРМ Это 60% от всех инцидентов на контролируемые ресурсы. На втором месте расположились атаки на web-серверы и иные сервисы.

Основные типы атак на веб — брутфорс и попытки эксплуатации уязвимостей, в том числе и на веб-сервер Apache. На пользовательские АРМ — вредоносное ПО, попытки эксплуатации уязвимостей в браузерах. Большое количество установленных нелегальным путём майнеров.

Центр мониторинга ЗАО «ПМ»

Отчёт подготовлен сотрудниками Центра мониторинга в сентябре 2018 года.

Сообщить о инциденте информационной безопасности и получить помощь в реагировании можно по ссылке — https://amonitoring.ru/incident/ или по телефону +7 495 737-61-97.

Описание всех услуг компании «Перспективный мониторинг» — https://amonitoring.ru/service/