ATLAS® Intelligence Feed

Более эффективные ответные меры на угрозы безопасности

Угрозы безопасности могут иметь различные проявления от нарушения функционирования сети до незаконного доступа к информации. В настоящее время предприятия должны постоянно следить за уровнем защиты от злоумышленников, которые хорошо организованы и крайне изобретательны. Современные угрозы являются вызовом как для сетевых администраторов и так и для администраторов информационной безопасности, поскольку сочетают различные типы целенаправленных атак, осуществляющихся в разное время и в различных точках сети. Организациям надо быстро и точно определить атаку, чтобы применить меры по ее предотвращению до того, как организация понесет потери.

Противодействие сложным угрозам

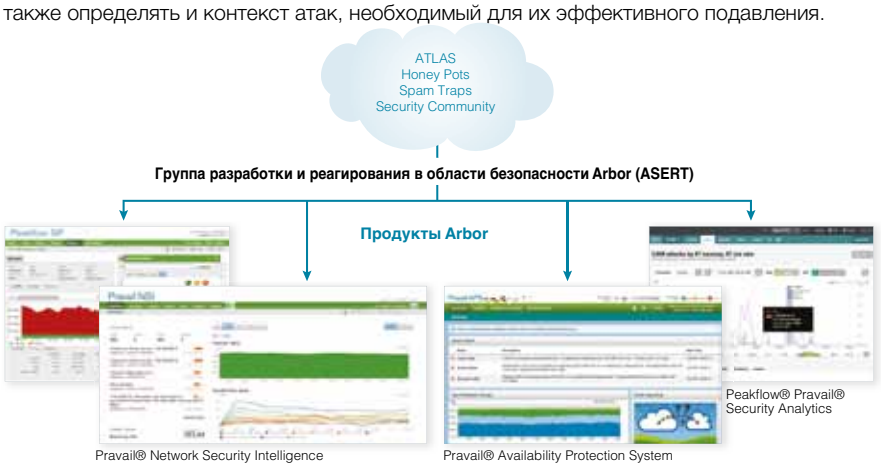
Продукт ATLAS Intelligence Feed от Arbor Networks обеспечивает клиентов политиками безопасности и противомерами, которые делают возможным быстро среагировать на единичные атаки как части сложной угрозы. ATLAS Intelligence Feed — это интеллектуальный продукт от исследовательской команды Arbor Networks – ASERT (Arbor Security Engineering and Response Team), дающий клиентам глубину и широту понимания проблем, свойственные научно-исследовательскому потенциалу Arbor.

У компании Arbor Networks богатое портфолио продуктов, разработанных как для предприятий, так и поставщиков сетевых услуг. Как только обнаруживается информация по новой атаке, ATLAS Intelligence Feed обновляется, и соответствующие изменения автоматически добавляются во все продукты Arbor посредством подписки на услугу через защищенный канал связи SSL, обеспечивая заказчиков последними технологиями защиты от угроз и препятствуя современным сложным атакам.

Динамика эффективности фида безопасности

Базы знаний и сигнатур хороши ровно на столько насколько хороша исходная информация, на основе которой они создаются. Меняющийся характер сложных атак создает необходимость в специальной группе по исследованию сетевой безопасности, имеющую в своем распоряжении самые современные технологии анализа не только вредоносного кода, но и полной организации атаки: как она была разработана, ресурсы для реализации и непосредственно приведение атаки в действие.

Команда мирового уровня компании Arbor по исследованию сетевой защиты вплотную занимается обнаружением и анализом возникающих Интернет-угроз, а также разработкой целенаправленных средств защиты. Для создание политик ATLAS Intelligence Feed (AIF) Arbor применяет сложные сочетание методов сбора данных об атаках, информацию от партнеров и средства анализа. Использование подписки AIF дает возможность не только детектировать современные информационные угрозы, но также определять и контекст атак, необходимый для их эффективного подавления.



Основные особенности и преимущества

Новейшая высококачественная защита

ATLAS Intelligence Feed (AIF) постоянно обновляется последними данными по сетевым угрозам, чтобы поддерживать самый точный механизм выявления потенциальных угроз во всех продуктах Pravail и Peakflow.

Разностороннее обнаружение атак

AIF использует информацию из различных источников, включая реальные данные по атакам через системы ATLAS, что дает возможность обнаружить сотни тысяч атак.

Быстрое реагирование на атаку

Политики AIF предоставляют ценную информацию о контексте каждой атаки, обеспечивая более быструю и убедительную реакцию на инциденты безопасности.

Анализ репутации на основе исследования

Информация о репутации применяется для быстрого и постоянного обновления AIF, чтобы легитимный трафик гарантировано не помечался как вредоносный.

ARBOR® NETWORKS

Как ATLAS Intelligence Feed защитит организации от DDoS-атак и ботнетов?

Многие клиенты Arbor Networks оценили ATLAS Intelligence Feed как эффективный программный инструмент для блокирования целенаправленных, комплексных и продвинутых атак.

Чтобы как можно точнее выявить сетевую угрозу, ATLAS Intelligence Feed (AIF) выполняет следующее:

- Определяет угрозу независимо от масштабов атаки; не ждет пока атака достигнет критического уровня, чтобы начинать меры по ее предотвращению.
- Использует многоуровневый способ защиты с учетом уровней доверия.
- Применяет опыт в сфере интеллектуальной защиты от угроз на основе продвинутых технологий по изучению разнообразного вредоносного ПО.
- Использует методы обратного инжиниринга вредоносных ПО и вирусов, связанных с бот-сетями.
- Круглосуточно мониторит Интернет-угрозы, используя глобальную сеть сенсоров компании Arbor.
- ATLAS — это совместный проект с более чем 300 клиентами, которые согласились анонимно делиться данными по трафику, что составляет существенную цифру в 90 Tbps или около одной трети всего Интернет-трафика.

Одной из ключевых технологий, лежащих в основе ATLAS Intelligence Feed, является динамическая оценка репутации объектов. Служба оценки репутации пополняет существующие данные в рамках работы ATLAS Intelligence Feed, чтобы пользователи не заходили на сайты с размещенными вредоносными элементами или функционирующих в качестве серверов управления бот сетями. В отличие от других решений служб оценки репутации, фид компании Arbor обновляется с большой частотой для максимального отслеживания быстро меняющегося поведения злоумышленников. Частое обновление помогает обеспечить более эффективное и точное выявление сетевых атак.

Другие важные преимущества ATLAS Intelligence Feed включают:

ATLAS

Основой преимущества компании Arbor на рынке является широкое сотрудничество с сервис-провайдерами, что помогает защите сетей наших клиентов. ATLAS — это совместный проект с более чем 300 клиентами, которые согласились анонимно делиться данными по трафику, что составляет существенную цифру в 130 Tbps или около одной трети всего Интернет-трафика. Благодаря своей уникальности Arbor позиционируется как лидер по предоставлению услуг сетевой защиты от DDoS атак , вредоносного ПО и бот-сетей, которые угрожают инфраструктуре и доступности сети. Клиенты Arbor пользуются прекрасной возможностью сочетать исследование сети в глобальном и локальном масштабе. На сегодняшний день такое мощное объединение ресурсов по защите от сетевых атак является непревзойденным примером решения в сфере безопасности.

Red Sky Alliance

Arbor Networks является основателем Red Sky® Alliance — закрытой социальной сети надежных экспертов по сетевой безопасности. Команда специалистов работает над методами выявления и нейтрализации вредоносного ПО и других продвинутых угроз. Члены сети Red Sky обмениваются действенными средствами защиты для эффективной борьбы с комплексными и скрытыми атаками, которые часто остаются незамеченными обычными схемами сетевой защиты. Защита от атак, разработанная Red Sky Alliance, улучшает основанную на данных ATLAS существующую защиту Arbor в режиме реального времени, обеспечивая уникальную видимость продвинутых атак, включая DDoS атаки.

Ключевые продукты по сетевой защите

Каждый продукт портфолио Arbor Networks нацелен на решение разнонаправленных проблем в зависимости от потребностей клиентов. Следует отметить, что несмотря на то, что все продукты могут работать с ATLAS Intelligence Feed, обработка данных происходит в зависимости от выбора продукта. Некоторые продукты обрабатывают NetFlow, другие берут в обработку данные сетевых пакетов. В описаниях продуктов должна быть указана соответствующая информация.

- **Pravail® Availability Protection System.** Помимо блокировки атаки при нарушении установленного порога Pravail APS использует данные системы ATLAS для обнаружения различных типов DDoS атак на уровне приложений. ATLAS Intelligence Feed позволяет Pravail APS найти и остановить воздействие на сеть определенных категории ботнетов. Предотвращение такой атаки до того, как пострадают критичные сервисы, позволяет устройствам безопасности выполнять свои функции.
- **Pravail® Network Security Intelligence.** Система защиты ATLAS Intelligence Feed выявляет инциденты, как только происходит нарушение политик защиты. Решение Pravail NSI позволяет организациям контролировать трафик и передачу информации между основными ресурсами и соответственно направлять на дальнейшее исследование в случае инцидентов.
- **Pravail® Security Analytics.** Политики AIF в рамках решения Pravail Security Analytics дают организациям инструмент анализа сетевой безопасности компании, обнаружения атак и расследования инцидентов. Индикаторы атаки предоставляют полезную информацию, какая атака обнаружена в сети (или была обнаружена ранее), а также на какой участок она распространилась. Следует отметить, что как только новые индикаторы добавились в ATLAS Intelligence Feed, поиск по существующим данным может перезапуститься для выявления подобных инцидентов в прошлом.
- **Peakflow®.** Сетевая защита от ATLAS Intelligence Feed обеспечивает клиентов решения Peakflow возможностью быстро выявить крупные DDoS атаки до того, как произойдет сбой в клиентской системе.
- **Peakflow® Threat Management System.** Политики AIF, используемые в Peakflow Threat Management System, предоставляют организации детальную информацию о DDoS атаках, их источниках, а также являются превосходными средствами для быстрой и надежной блокировки. Такая четкость критична в блокировке атак вредоносного ПО, проникновение которых может привести к дорогостоящим простоям системы.

Элементы системы защиты

ATLAS Intelligence Feed доступен в двух версиях — Standard и Advanced. Используя одну из двух подписок, клиент может выбирать уровень выявления атак и/или защиту в соответствии со своими требованиями.

ATLAS Intelligence Feed Standard

Используя AIF Standard, клиент может определять и/или устранить самые основные атаки на сегодняшний день, включая вредоносное ПО, ботнеты и отказы сервисов. Политики и противомеры постоянно обновляются для обеспечения полного, аккуратного обнаружения новых атак. Примеры политик и мер по предотвращению по версии продукта Standard указаны ниже:

Category	Sub-Category of Threats		Pravail			Peakflow	
			APS	NSI	SA	SP	TMS
Command and Control	• Peer to Peer • HTTP • IRC		◉	◉	◉	◉	
DDoS Reputation Threats	• Attacker • Target		◉	◉	◉	◉	
Malware	• Webshell • Ransomware • RAT • Fake Anti Virus • Banking • Virtual Currency • Spyware • Drive By • Social Network	• DDoS Bot • Dropper • Ad Fraud • Worm • Credential Theft • Backdoor • Other • Exploit Kit • Point of Sale	◉	◉	◉	◉	
IP Geo Location	• Identify location by country for sources of inbound • Identify location by country for destinations of outbound traffic		◉		◉	◉*	◉*
DDoS RegEx	• Identifies DDoS attackers based upon IP address indicators from ATLAS • Identifies DDoS targets based on indicators from ATLAS HTTP Flooder		◉				◉
Web Crawler Identification	• Identify inbound connections to web services from known search engines		◉				
ET Pro *Comes standard with SA deployments*	• IDS Signatures				◉		

Рисунок 1. Пример угрозы, выявленной версией AIF Standard. Все противомеры и политики постоянно обновляются, поэтому вышеупомянутый перечень может меняться в любой момент.

*IP геолокация обновляется в SP и TMS решениях через патч.

Как уникальные возможности Arbor Networks помогают в разрешении продвинутых угроз

У компании Arbor богатый опыт в исследовании ботнетов и предотвращения DDoS атак. Несмотря на то, что DDoS-атаки стали частью вредоносного ПО и ботнетов, участвующих в киберпреступлениях и APT атаках, компания Arbor ориентирует команду ASERT и свои исследовательские ресурсы, чтобы блокировать угрозы новых типов.

Существует несколько функций, которые позволяют группе ASERT обнаруживать вредоносный трафик, включая целенаправленные атаки. Эти функции включают:

- Ценное партнерство, такое как Red Sky Alliance, которое имеет доступ к более чем 23 миллионам ПК, которые активно контролируются на предмет защиты.
- Проверка репутации и активный трекинг атак на основе реальных показателей, предоставленных Red Sky Alliance.
- Тщательный анализ вредоносного ПО включает как внешние партнерские технологии, так и результаты внутреннего анализа и обработки данных.

ASERT использует данные по угрозам и результаты анализа, чтобы улучшить работу ATLAS Intelligence Feed, к которому обращаются клиенты компании Arbor для обнаружения инцидентов внутри и вне сети. Объединение локального (в рамках сети) и глобального (предоставленные данные с портала ATLAS) исследования трафика дает клиентам возможность быстрого реагирования на продвинутые угрозы.

ATLAS Intelligence Feed Advanced

ATLAS Intelligence Feed Advanced разработан для организаций, которых волнуют скрытые и непроявленные атаки. С подпиской на это обновление клиент получает помимо базы противомер и политик из AIF Standard еще и дополнительные политики, позволяющие обнаружить большой спектр APT-атак. В этом варианте освещаются атаки, созданные специально для определенных предприятий. Их сложно отследить, так как атаки маскируются под легитимный трафик. Примеры противомер и политик, включенных в подписку на AIF Advanced.

Category	Sub-Category of Threats	Pravail			Peakflow	
		APS	NSI	SA	SP	TMS
Location Based Threats	• Traffic Anonymization Services • TOR • Proxy • Sinkholes • Scanner • Other	◉	◉	◉		
Email Threats	• Spam • Phishing	◉	◉	◉		
Targeted Attacks	• APT • Hacktivism • RAT • Watering Hole • Rootkit	◉	◉	◉		
Mobile	• Mobile C&C • Spyware • Malicious App	◉	◉	◉		

Рисунок 2. Пример угрозы, выявленной версией AIF Standard. Все противомеры и политики постоянно обновляются, поэтому вышеупомянутый перечень может меняться в любой момент. В настоящее время подписка на версию Advanced недоступна для продуктов Peakflow или Peakflow Threat Management System customers.

Центральный офис компании

76 Blanchard Road
Burlington, MA 01803 USA
Тел. (бесплатно для США):
+1 866 212 7267
Тел. +1 781 362 4300

Отдел продаж в Северной Америке

Тел. (бесплатный звонок):
+1 855 773 9200

Европа

Тел. +44 207 127 8147

Азиатско-тихоокеанский регион

Тел.: +65 68096226

www.arbornetworks.com

DS/MNA/EN/0914-LETTER

Arbor Networks обеспечивает защиту крупнейших мировых компаний и провайдеров связи от DDoS-атак и других угроз безопасности. По данным исследований Infonetics Research компания Arbor Networks является основным поставщиком решений по предотвращению распределенных атак типа DoS как в корпоративном и операторском сегментах, так и среди поставщиков мобильных сервисов. Передовые решения компании Arbor по отражению угроз обеспечивают максимальную прозрачность сетевых процессов посредством сочетания технологии NetFlow и сбора пакетов, что позволяет быстро обнаруживать и обезвреживать внутренние вредоносные программы и пакеты данных. Компания Arbor также занимает лидирующие позиции на рынке поставщиков аналитики для оперативного реагирования на угрозы, исторического анализа, визуализации и криминалистической экспертизы. Компания Arbor прикладывает все усилия, чтобы предоставить своим клиентам максимально защищенные сети основываясь на опыте команд-экспертов в области безопасности. Наша цель состоит в привнесении большей ясности и контекста безопасности в современную сетевую инфраструктуру. Это приведет к более оперативному решению проблем заказчиков и снижению рисков для их бизнеса.