Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Программный блейд Anti-Bot
Первое интегрированное сетевое решение Anti-Bot – усиленное ThreatCloud™

Программный блейд Anti-Bot

ЧТО ТАКОЕ БОТ?

Бот – это вредоносная, скрытая программа, которая проникает в вашу сеть и позволяет злоумышленникам удаленно управлять вашим компьютером. Киберпреступники могут удаленно осуществлять незаконную деятельность, такую как кража данных, рассылка спама, распространение вредоносных программ и участие в атаках Отказа в обслуживании (DoS) без вашего ведома. Боты играют ключевую роль в целевых атаках также известных как Расширенные стойкие угрозы (APT). Для защиты вашей компании от подобных атак необходимо многоуровневое интегрированное решение предотвращения угроз.

ОБЗОР ПРОГРАММНОГО БЛЕЙДА CHECK POINT ANTI-BOT

Программный блейд Check Point Anti-Bot обнаруживает бот-инфицированные машины и предотвращает деятельность бота путем блокирования соединений от серверов «Команд и Управления» (C&C) злоумышленника. Используя постоянно обновляемый список C&C-адресов из ThreatCloud™, крупнейшей, работающей в режиме реального времени, базы знаний угроз безопасности из «облака», Программный блейд Anti-Bot обнаруживает скрытых ботов прежде, чем они смогут нанести ущерб, и затронут пользователей.

РЕШЕНИЕ ДЛЯ БОТОВ

Решение Check Point Threat Prevention, в том числе Программный блейд Ant-Bot, подпитываются сетью ThreatCloud™, которая снабжает шлюз безопасности вторым уровнем интеллектуальной защиты с более чем 250 миллионов адресов проанализированных на наличие ботов, более 4,5 млн. сигнатур вредоносных программ и более 300,000 инфицированных вредоносным ПО web-сайтов.

THREATCLOUD™

ThreatCloud – первая объединенная сеть для борьбы с киберпреступностью. Она, в режиме реального времени, динамически обеспечивает данные о безопасности шлюзам безопасности. Эти данные используется для выявления новых атак и тенденций угроз. ThreatCloud питает Программный блейд Anti-Bot, позволяя шлюзам собирать сведения о постоянно меняющихся IP, URL и DNS адресах известных центров Управления и Контроля. Поскольку обработка выполняется с применением облачных технологий, миллионы сигнатур и защита от вредоносного ПО могут быть отсканированы в режиме реального времени.

ФУНКЦИИ

Первое интегрированное сетевое решение Anti-Bot

- Защита даже после инфицирования через обнаружение ботов и остановку их деятельности
- Единое управление, отчетность и политики с Программным блейдом Antivirus
- Доступно для всех шлюзов

Усиленное ThreatCloud™

ThreatCloud – первая объединенная сеть для борьбы с киберпреступностью, которая снабжает программные блейды шлюза безопасности интеллектуальной защитой в режиме реального времени

- 250 миллионов адресов проанализированы на наличие ботов
- 4,5 миллиона вредоносных сигнатур
- 300,000 вредоносных web-сайтов

ThreatSpect™– многоуровневый движок обнаружения бота

Обнаруживает инфекции путем сопоставления различных методов обнаружения бота

- Репутация IP-адресов, URL-адреса и DNS-адресов
- Шаблоны обнаружения бот-соединений
- Сканирование на активность бота
- Единая защита и управление интегрированы с программным блейдом Anti-Bot
- Централизованно управляемый с единой пользовательской консоли

ПРЕИМУЩЕСТВА

- Выявляет боты, которые проникли на ваши компьютеры
- Прекращает APT-атаки
- Предотвращает ущерб, такой как кража данных
- В курсе постоянно меняющегося динамического ландшафта угроз, получая информацию в режиме реального времени от ThreatCloud
- Легко исследует инфекции, оценивает ущерб и принимает решение о последующих шагах с помощью расширенных средств экспертизы
- Просмотр и управление «большой злобной картинкой» со встроенными отчетами об угрозах и информационными панелями

Программный блейд Anti-Bot

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

База знаний ThreatCloud динамически обновляется, используя информацию об атаках со шлюзов по всему миру, подпитывается из сети глобальных датчиков угроз, научно-исследовательских лабораторий Check Point и лучших в отрасли вредоносных каналов. Коррелированная информация об угрозах безопасности затем коллективно распределяется между всеми шлюзами.

ThreatSpect™– движок поиска бота

Боты незаметны, часто скрываются на вашем компьютере не выявляемые распространенными антивирусными программами. Программный блейд Check Point Anti-Bot обнаруживает бот-инфицированные машины при помощи собственного движка ThreatSpect™, уникальная многоуровневая технология обнаружения с самыми современными обновлениями поступающими из ThreatCloud. ThreatSpect коррелирует информацию для точного обнаружения бота.

- Адреса удаленного управления, включая IP, DNS и URL-адреса
- Обнаружение уникальных шаблонов соединений ботнета
- Обнаружение атак, таких как спам или «кликовое мошенничество»

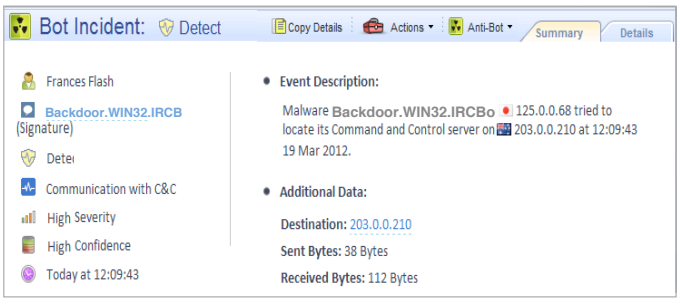
Блокировать соединения бота

После обнаружения бота, Программный блейд Check Point Anti-Bot блокирует команду на создание удаленного соединения между зараженной машиной и C&C сервером, тем самым делает бот бесполезными для злоумышленников и защищает организацию от возможного ущерба действиями бота.

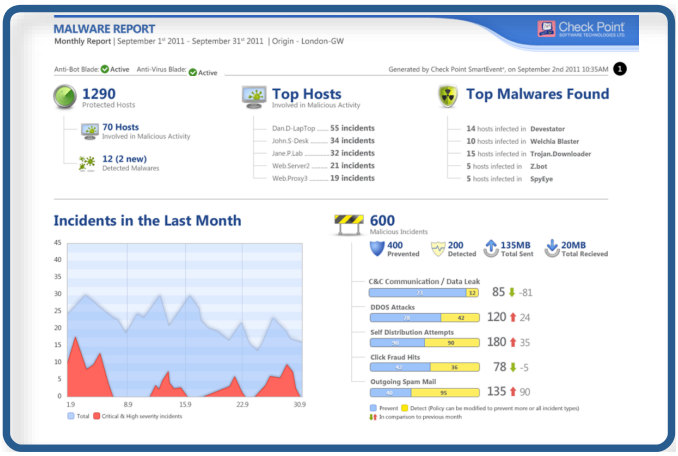
Расследование инфицирования ботами

Уверенно распознавать бот-инфекции в расширенных журналах регистрации и системой управления, обеспечивающих ключевыми ресурсами, такими как зараженный компьютер/пользователь, название бота, действия бота (например, связь с C&C и рассылка спама), объем переданных/полученных данных, серьезность инфекции и многое другое.

Кроме того, решение включает в себя всеобъемлющий ThreatWiKi позволяющий команде по обеспечению безопасности легко понять, с каким ботом они сталкиваются, что он делает, как он работает и получить любую другую техническую информацию.



Всесторонняя экспертиза.



Вид «большой злобной картинки» со встроенными отчетами об угрозах.

Единая защита от ботов и вредоносного ПО

Программный блейд Anti-Bot объединенный с программным блейдом Antivirus предоставляет защиту организациям как до, так и после заражения и обеспечивает многоуровневое предотвращение угроз. Администраторы управляют едиными политиками и отчетами, и все это в одном пользовательском интерфейсе.

Интегрирован в Check Point Архитектуру «Программные блейды»

Программный блейд Anti-Bot полностью интегрирован в Архитектуру «Программные блейды» – экономит время и снижает затраты, позволяет клиентам быстро расширить уровень защиты в соответствии с изменяющимися требованиями. Его можно просто и быстро активировать на имеющихся шлюзах безопасности Check Point, экономя время и снижая затраты за счет использования существующей инфраструктуры безопасности. Программный блейд Anti-Bot имеет централизованное управление, позволяет центральное администрирование политики, принудительное применение и регистрацию с помощью единственной удобной консоли.

ХАРАКТЕРИСТИКИ ПРОГРАММНОГО БЛЕЙДА

Поддерживаемые семейства устройств

- Check Point Устройства 2200, 4000, 12000, 21400 и 61000*
- Check Point Power-1
- Check Point Устройства IP
- Check Point UTM-1
- Check Point IAS

Поддерживаемые ОС

- GAiA
- SecurePlatform
- IPSO 6.2 на HDD
- Windows

*2H/2012

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com
Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com