Internet Engineering Task Force (IETF)
Request for Comments: 6018
Category: Informational
ISSN: 2070-1721

F. Baker
Cisco Systems
W. Harrop
G. Armitage
Swinburne University of Technology

September 2010

IPv4 and IPv6 Greynets

«Серые» сети IPv4 и IPv6

Аннотация

В этом документе рассматривается модель построения «серых сетей» (Greynet) для IPv4 и IPv6.

Статус документа

Этот документ не является спецификацией стандартного протокола Internet и опубликован лишь для информации.

Документ является результатом работы IETF[1] и выражает согласованное мнение сообщества IETF. Документ был вынесен на общее рассмотрение и одобрен для публикации IESG[2]. Не все документы, одобренные IESG, рассматриваются в качестве возможных стандартов Internet того или иного уровня (см. раздел 2 в RFC 5741).

Информацию о статусе документа, обнаруженных в нем ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc6018.

Оглавление

1. Введение

«Темные сети»[3] или «сетевые телескопы» развернуты несколькими организациями (включая CAIDA, Team Cymru и Мичиганский университет) для наблюдения за трафиком, адресованным в реально не используемые блоки адресов. Такой трафик становится видимым путем прямого сбора (маршрутизации в коллектор) или благодаря откликам на него (пакеты ICMP или пакеты сброса на транспортном уровне).

С темными сетями связаны две проблемы. Как только их адреса становятся известными, атакующие прекращают использование этих адресов, что ведет к снижению эффективности темных сетей. Кроме того, администраторы таких сетей связаны правилами региональных регистраторов Internet (RIR[4]) и требованиями бизнеса, что препятствует развертыванию темных сетей в активных сетях.

В работе [Harrop] введено понятие «серой сети» (Greynet):

> Темные сети часто предлагаются для мониторинга аномального трафика из внешних источников и для таких сетей требуются большие непрерывные блоки неиспользуемых адресов IP - выделение таких блоков зачастую нежелательно для операторов. Мы разработали и опробовали «серую сеть» - «светлый» (lit) диапазон адресного пространства IP, в котором достаточно редко встречаются адреса темных сетей, а большую часть пространства занимают активные («светлые») адреса IP. На основе небольшой выборки трафика в кампусной сети университета можно сказать, что относительно малая плотность темных сетей позволяет обеспечить достаточно эффективное обнаружение сканирования сетей.

[1] Internet Engineering Task Force.
[2] Internet Engineering Steering Group/
[3] Darknet.
[4] Regional Internet Registry.

Иными словами, вместо резервирования префиксов, которые злоумышленники смогут попытаться проверить, рискую быть обнаруженными, Harrop предложил отвести для этого отдельные адреса (или небольшие группы смежных адресов) в подсетях, используя разные идентификаторы хостов в каждой подсети для осложнения сканирования адресов с целью обнаружения. Концепция имеет ценность в том смысле, что осложняет сопоставление адресов или префиксов с шаблоном поиска злоумышленника, поскольку их присутствие менее очевидно. В исследовании Harrop использовался протокол IPv4 [RFC0791] и была получена интересная информация.

1.1. Предыстория

Исследование, поддерживающее это предложение, включает 2 прототипа - один для IPv4 [RFC0791], другой для IPv6 [RFC2460]. Оба имеют ограничения, будучи исследовательскими экспериментами, а не реализацией готового решения.

Исходное исследование выполнил Warren Harrop и описал в [Harrop]. Оно проводилось лишь для IPv4. Автор исходил из того, что в ЛВС можно разместить неиспользуемую виртуальную или физическую машину, которая будет служить для обнаружения разных типов сканирования. Как отмечено в упомянутой статье, концепция эффективно работала при развертывании прототипа в Центре современной архитектуры Internet (CAIA[1]) Swinburne University of Technology. Основная причина заключалась в том, что со стороны возможного злоумышленника разумно было ожидать присутствия этого адреса и не было шаблонов, которые бы позволили тому догадаться о способе применения машины. В CAIA был разработан и выпущен прототип основанной на FreeBSD системы Greynet в 2008 г. [Armitage].

Baker добавил в свою концепцию маршрутизатор с идеей о том, что тот с большой вероятностью увидит любое сканирование, если оно пришло извне локальной сети и маршрутизатор должен будет использовать протокол ARP[2] или ND[3] для идентификации (или отказа при попытке идентификации) интересующей злоумышленника машины. По сути дела, любой отсутствующий в подсети адрес действует как триггер Greynet. Очевидно, что это будет работать в любой системе, которая реализует ARP или ND, но маршрутизатор обычно служит точкой входа в любую подсеть.

Tim Chown из School of Electronics and Computer Science University of Southampton предложил в частном порядке провести некоторые исследования по этому вопросу и весной 2010 г. Owen Stephens сделал для этого прототип Linux. Они продемонстрировали, что технология проста в реализации и фактически работает на прототипе реализации IPv6.

Вопрос, остающийся при сканировании адресов IPv6, заключается в вероятности того, что атака произойдет. Chown изначально утверждал в [RFC5157], что сканирование адресов было невозможно по причине слишком большого их числа. Однако в сентябре 2010 г. был выпущен отчет NANOG о сканировании адресов IPv6. Кроме того, имеются способы ограничения области сканирования, например, можно увидеть, что компания покупает определенный тип машин или сетевых плат (NIC[4]) и поэтому ее вероятные адреса EUI-64 ограничены диапазоном, который меньше 2^{64} и больше похоже на 2^{24} адресов в данной подсети или можно наблюдать DNS, конверты SMTP, сообщения XMPP[5], FTP, HTTP и т. п., где содержатся адреса IP. Такие атаки можно ограничить использованием адресов Privacy Addresses [RFC4941], которые периодически меняются, делая прошлую информацию менее полезной. Однако такие аналитические методы существуют.

2. Развертывание серых сетей

Корпоративные отделы IT и другие операторы сетей часто применяют коллекторы и другие типы датчиков. Коллектор - это компьютерная система в Internet, которая специально настроена для привлечения и «отлова» пытающихся проникнуть в систему. Такие средства могут просто записывать попытки или дейтаграммы, инициирующие попытку (darknet/Greynet), или могут служить приманкой для атак с целью изучения действий и методов (honeypot - ловушка).

Для решения этой задачи вредоносный трафик отделяется от представляющегося обычным и нужным с целью изучения одного и облегчения другого.

2.1. Развертывание с использованием маршрутизации - темные сети

Одним из очевидных способов идентификации и изоляции вредоносного трафика является его направленность на несуществующие адреса или префиксы. Если в кампусе используется сеть IPv4 с префиксом /24 или IPv6 с префиксом /56, но реально применяется меньше 100 подсетей, можно, например, использовать только четные подсети (128 из 256 для указанного префикса). Зная, что активные префиксы более специфичны и поэтому привлекают соответствующий трафик, можно анонсировать из коллектора используемый по умолчанию префикс, привлекая трафик на неиспользуемые префиксы данного домена.

Второй вопрос связан с имитацией атакуемого хоста - коллектор может просто записывать незванный трафик, а может отвечать на него как ловушка (honeypot).

2.2. Использование малозаселенного адресного пространства - «серые сети»

В подсетях IPv4 обычно имеются нераспределенные адреса, хотя бы потому, что в бесклассовой междоменной маршрутизации (CIDR[6]) выделяются блоки адресов $O(2^n)$, размер которых не всегда совпадает с числом систем в подсети. Так же происходит с активными префиксами IPv6 и даже в очень большой коммутируемой ЛВС скорей всего будет использована лишь часть адресов. Этот вопрос рассматривается в параграфе 2.5.1 [RFC4291]. Если адреса распределены более или менее случайно, вероятность того, что атакующий угадает реально применяемые адреса, достаточно мала. Это позволяет использовать такие незанятые адреса внутри префикса IP.

Маршрутизаторы применяют IPv4 ARP [RFC0826] и IPv6 Neighbor Discovery [RFC4861] для определения адресов MAC (Media Access Control - управление доступом к среде) своих соседей, которым нужно передавать дейтаграммы. Обе спецификации предполагают, что при поступлении дейтаграммы на маршрутизатор, обслуживающий целевой префикс, но не знающий MAC-адреса предполагаемого получателя, тот будет выполнять ряд действий:

---

[1] Centre for Advanced Internet Architectures.
[2] Address Resolution Protocol - протокол преобразования адресов.
[3] Neighbor Discovery - обнаружение соседа.
[4] Network interface card.
[5] Extensible Messaging and Presence Protocol - расширяемый протокол сообщений и присутствия.
[6] Classless Inter-Domain Routing.

- размещение дейтаграммы в очереди;
- передача запроса Neighbor Solicitation или ARP;
- ожидание отклика Neighbor Advertisement или ARP;
- при получении отклика пересылка дейтаграммы из очереди.

Когда MAC-адрес хоста имеется в таблице маршрутизатора (и является действительным) вопросов не возникает.

В статье [Harrop] серая сеть (Greynet) организуется на хосте, который отвечает на запросы ARP для всех «темных» адресов IP. Однако небольшое изменение в маршрутизаторе может дополнить эту модель. Помимо постановки в очередь или отбрасывания дейтаграммы, вызвавшей запрос ARP или Neighbor Solicitation, маршрутизатор копирует ее через независимый канал к оборудованию Greynet. Этот канал может быть отдельным физическим интерфейсом, устройством, VLAN, туннелем, инкапсуляцией UDP (или иной), а фактически любым местом, где такая дейтаграмма может быть обработана. В зависимости от требований приемного коллектора можно также предоставлять суммарную информацию в виде IPFIX[1] [RFC5101] [RFC5610].

Анализирующее оборудование будет получать два типа дейтаграмм. Наиболее интересны будут те, которые направлены по «темным» адресам IP. Менее интересен случай, когда дейтаграмма адресована легитимному узлу, MAC-адрес которого по той или иной причине временно отсутствует в таблице маршрутизатора. Дейтаграммы, прибывающие адресатам IP, для которых отклик ARP (или Neighbor Advertisement) еще не получен, также могут пересылаться анализирующему устройству по независимому каналу, но это вряд ли даст полезную информацию.

Анализирующее оборудование, в зависимости от способа распознавания маршрутизатором «темных» адресов IP, может легко отслеживать картину дейтаграмм, направленных в неиспользуемые части сети. Оно также может отвечать на такие дейтаграммы, выступая в качестве применки для получения дополнительных дейтаграмм от атакующего.

Если коллектор отвечает напрямую, атакующий может обнаружить это с помощью информации из дейтаграммы (или о ней) - например, дейтаграммы, отправленные в ту же подсеть IP, могут приходить с другими значениями TTL. Поэтому для коллектора может оказаться разумным ответ через туннель, как будто ответ пришел из той же подсети IP. В этом случае коллектору не следует отвечать на дейтаграммы, направленные по «светлым» адресам IP, поскольку исходный получатель в конечном итоге ответит на ARP или Neighbor Solicitation.

Одним из следствий этой модели является то, что распределенные DoS-атаки (DDoS[2]) завершаются в подсетях маршрутизатора, а не на каналах между маршрутизаторами.

2.3. Другие фильтры

Очевидное расширение концепции будет включать трафик, идентифицируемый другими фильтрами, для передачи коллектору. Например, можно настроить систему на пересылку трафика, для которого не проходит проверка по обратному пути с индивидуальной маршрутизацией (uRPF[3]) [RFC2827], в коллектор через тот же туннель.

3. Влияние на устройство маршрутизаторов

Влияние на устройство маршрутизаторов относится к алгоритмам IPv4 ARP и IPv6 Neighbor Discovery. Может оказаться интересной (настраиваемая в конфигурации) возможность пересылки в анализирующую систему приходящих дейтаграммы, которые вызывают запросы ARP Request или Neighbor Solicit, приводящие к отказу, в интерфейс, устройство, VLAN или туннель.

4. Вопросы безопасности

Этот документ описывает средство для поддержки безопасности сетей IPv4 и IPv6. Подобно другим инструментам, оно имеет ограничения и возможные атаки. Если отбрасывание трафика в условиях перегрузки - вещь хорошая, то его удержание и последующая пересылка создают нагрузку на сеть и маршрутизатор, что может служить для организации атаки. Однако для такой атаки имеется очевидное смягчение - просто выбирается (как удобно для оператора) подмножество пересылаемого трафика и отбрасывается остальной. Кроме того, такие атаки не новы, здесь лишь меняется характер. Поток, который будет создавать атаку, приведет к росту числа сообщений ARP или Neighbor Solicit, которые все принимающие хосты должны отбрасывать. Такая атака занимает часть пропускной способности, но здесь эта часть предполагается выделенной специально.

Вопрос о доле интересующего и экономически оправданного трафика для пересылки намеренно оставлен открытым. Ключевые вопросы разработки включают возможность получения информации из сделанной выборки (наблюдаются ли пики трафика? Если да, то что он собой представляет?), влияние на маршрутизаторы и другое вовлеченное оборудование, способы смягчения этого влияния и т. п. Возможные алгоритмы выбора, зависящие только от состояния и алгоритмов, которые обычно доступны доступны в маршрутизаторах, перечислены ниже.

- Выбор всех дейтаграмм, вызывающих ARP Request или Neighbor Solicit.
- Выбор подмножества дейтаграмм, на которые не было ответа в течение некоторого заданного интервала времени (эти адреса вероятно являются «темными»).
- Выбор из этих адресов подмножества новых - если адрес был запрошен, пересылка избыточных данных может оказаться бесполезной.
- Выбор всех дейтаграмм с ограничением скорости.
- Выбор всех дейтаграмм, соответствующих (не соответствующих) определенному правилу фильтрации.

[1] IP Flow Information Export - экспорт информации IP Flow.
[2] Distributed denial-of-service.
[3] Unicast Reverse Path Forwarding.

5.Благодарности

Алгоритмы изучения поведения Internet-атак путем наблюдения рассеянного трафика использовались Team Cymru из CAIDA, University of Michigan и другими исследователями. Harrop расширил их в своем исследовании. Эта формулировка идеи обсуждалась авторами в 2005 г. Данный документ возник в результате разговора с Paul Vixie и Rhette Marsh о сенсорах трафика Internet, они также внесли полезные комментарии по этому поводу. Albert Manfredi отметил различие между ЛВС (в соответствии с IEEE 802) и подсетью IP.

Tim Chown [RFC5157] заметил, что, по крайней мере на момент написания этого RFC, об атаках со сканированием адресов для IPv6 не было известно. Однако, как отмечено в параграфе 1.1, об атаке с (частичным) сканированием недавно писали в почтовой конференции NANOG. Однако Rhette Marsh предложила структуру такой атаки, а Fred Baker - подходы, основанные на адресной информации, которой обмениваются приложения. Поэтому авторы считают, что такие проблемы могут возникнуть для IPv6 в будущем, когда IPv6 станет более интересной целью.

Tim Chown и Owen Stephens проверили предложение и внесли полезные комментарии, которые были включены в этот документ. Однако самым значительным их комментарием было: «Это работает».

6. Литература

6.1. Нормативные документы

[Harrop] Harrop, W. and G. Armitage, "Greynets: a definition and evaluation of sparsely populated darknets", IEEE LCN IEEE 30th Conference on Local Computer Networks, 2005.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

6.2. Дополнительная литература

[Armitage] Armitage, G., Harrop, W., Heyde, A., Parry, L., "Greynets: Passive Detection of Unsolicited Network Scans in Small ISP and Enterprise networks", CAIA, Swinburne University of Technology, December 2008, http://caia.swin.edu.au/greynets/.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5157] Chown, T., "IPv6 Implications for Network Scanning", RFC 5157, March 2008.

[RFC5610] Boschi, E., Trammell, B., Mark, L., and T. Zseby, "Exporting Type Information for IP Flow Information Export (IPFIX) Information Elements", RFC 5610, July 2009.

Адреса авторов

Fred Baker
Cisco Systems
Santa Barbara, California 93117
USA
EMail: fred@cisco.com

Warren Harrop
Centre for Advanced Internet Architectures
Swinburne University of Technology
PO Box 218
John Street, Hawthorn,
Victoria, 3122
Australia
EMail: wazz@bud.cc.swin.edu.au

Grenville Armitage
Centre for Advanced Internet Architectures
Swinburne University of Technology
PO Box 218
John Street, Hawthorn,
Victoria, 3122
Australia
EMail: garmitage@swin.edu.au

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru