Вестник ЦЭМИ РАН. 2013-2020

ISSN 2658--3887

URL - http://cemi.jes.su

Все права защищены

Выпуск 3 Том . 2019

Паразитный трафик Интернета: жизненный цикл атаки GRE-пакетами

Ляпичева Н. Г.
Центральный экономико-математический институт РАН
Москва, Нахимовский проспект, 47

Аннотация

На основе запротоколированных данных рассматривается жизненный цикл сетевой атаки GRE-пакетами и ее влияние на интернет-трафик. Отмечается роль СМИ на развитие и завершение жизненного цикла. Отмечена целесообразность запретительной политики доступа из Интернета.

Ключевые слова: компьютерные сети, сетевая безопасность, сканирование сетей, устройство защиты , жизненный цикл атаки

Дата публикации: 07.02.2020

Ссылка для цитирования:

Ляпичева Н. Г. Паразитный трафик Интернета: жизненный цикл атаки GRE-пакетами // Вестник ЦЭМИ РАН. 2019. Выпуск 3 [Электронный ресурс]. Доступ для зарегистрированных пользователей. URL: https://cemi.jes.su/s265838870007146-3-1/ (дата обращения: 10.02.2020). DOI: 10.33276/S265838870007146-3

1 **Предмет изучения.** С начала 2000-годов зафиксировано, что Интернет перенасыщен паразитным трафиком, порожденным постоянно ведущимися вредоносными действиями ряда пользователей. Это явление порождено как осознанными, специально организованными атаками (реже – направленными персонально на некоторую сеть, чаще – широковещательно, при помощи различных программных автоматов), так и последствиями халатности и легкомысленного отношения обычных пользователей к защите своих ПК от вредоносных кодов. Пример анализа таких последствий приведён в работах[1] [2], в которых исследована

активность почтовых вирусов в упомянутый период и приведены некоторые результаты.

2 Паразитный трафик, порождённый сканированием сетей по спискам ip-адресов с целью поиска доступных для воздействия открытых портов, уже не считается чем-то экстраординарным. В рядовом случае он не требует изучения и реагирования помимо стандартной функции брандмауэра 惆 именно в связи с необыкновенной распространённостью этого варианта сетевой атаки. Поэтому практически во всех системах обнаружения сетевых атак предоставляется возможность исключения из протоколирования части признаков (сигнатур) наиболее распространённых атак, не отменяя их опознания и отражения при возникновении такой необходимости[3]

3 В данной работе рассматривается жизненный цикл одного варианта атаки: возникновение и развитие сканирования сети по протоколу 47 (GRE)[4]] [5]] , направленного широкому кругу ip-адресов.

4 Протокол GRE - протокол туннелирования , разработанный компанией Cisco для инкапсулирования различных протоколов внутри ip-туннелей с целью создания виртуальных соединений «точка-точка». Специалисты, занимающиеся внедрением приложений, использующих данный протокол, отмечают такие характеристики протокола GRE как недостаточную защищенность его полезной нагрузки и отсутствие механизмов отслеживания состояния[6].

5 Чаще всего он используется в следующих целях:

- в сочетании с Point-to-Point Tunneling Protocol, (PPTP) - для создания виртуальных частных сетей (VPN);
- в технологии Wireless Distribution System (WDS) - для координации действий точек доступа и контроллера беспроводных сетей.
- в технологиях мобильного IP.

6 Таким образом, возможным конечным результатом данного рода атаки предполагалось обнаружение в сканируемых сетях слабозащищённых точек доступа с целью последующего их несанкционированного использования в нелегитимных целях.

7 Интерес к предмету изучения был вызван тем, что в отличие от упомянутых ранее (а также множества других неупомянутых) вариантов сканирования этот инцидент имеет точную дату первоначального обнаружения в сети ЦЭМИ РАН, защищенной брандмауэром, и запротоколированные количественные данные о предпринятых атаках.

8 **Сбор данных о паразитном трафике**. Исследование проводилось на главном маршрутизаторе института, представляющем собой специализированное устройство – ASA5510-R8, являющееся брандмауэром и выполняющем соответствующие функции[7].. В результате его функционирования атаки по протоколу 47 обнаруживались и гасились на брандмауэре ASA5510-R8, не вызывая серьезных проблем в сети и не требуя дополнительных действий, как это и определяется сообщением уровня «Error» с номером ASA-session-3-106010. Основным результатом воздействия на сеть стало отображение паразитного трафика GRE-пакетов в протоколе маршрутизатора и использование ресурсов сети для отражения атак и протоколирования.

9 Протоколирование и первичная обработка записей протоколов, относящихся к исследуемому явлению, проводилось на специально настроенном сервере, в период декабрь 2016 г. – июль 2017 г. Кроме того, были ретроспективно проанализированы записи протоколов с августа по декабрь 2016 г., что позволило обнаружить единичное сканирование в ноябре 2016 г.

10 **Графическое отображение жизненного цикла атаки.** Первое появление паразитного трафика GRE-пакетов было отмечено в августе 2016 г., воздействие на сеть ЦЭМИ РАН продолжалось 5 дней и не было достаточно активным для влияния на ее работу. Затем произошла одиночная попытка в ноябре того же года.

11 Таблица.

Дата	Зафиксировано попыток
2016, Август 04, четверг	17
2016, Август 05, пятница	8
2016, Август 06, суббота	15
2016, Август 07, воскресенье	5
2016, Август 08, понедельник	11
XXXXXXXXXXXXXXXXX	0
	Новое появление
2016, Ноябрь 02, Среда	6
XXXXXXXXXXXXXXXXX	0

12 Окончательный старт появившегося нового варианта сканирования произошел в декабре 2016 г., после чего паразитный трафик GRE-пакетов быстро набрал мощность (см. диаграмму, рис.1.). На пике своей активности он превосходил 8000 пакетов в сутки, неравномерно распределяясь в этот период.

13 Использование данного метода сканирования нарастает, пока он является новым и перспективным, и далее постепенно снижается интерес к данной активности по мере недостаточного успеха его использования. К концу мая 2017 г.объемы паразитного трафика GRE-пакетов достаточно стабилизировались, и составляли 400-500 попыток в сутки с постепенным дальнейшим снижением, однако не прекращаются поныне, как и вся нелегитимная активность в Интернете.

14

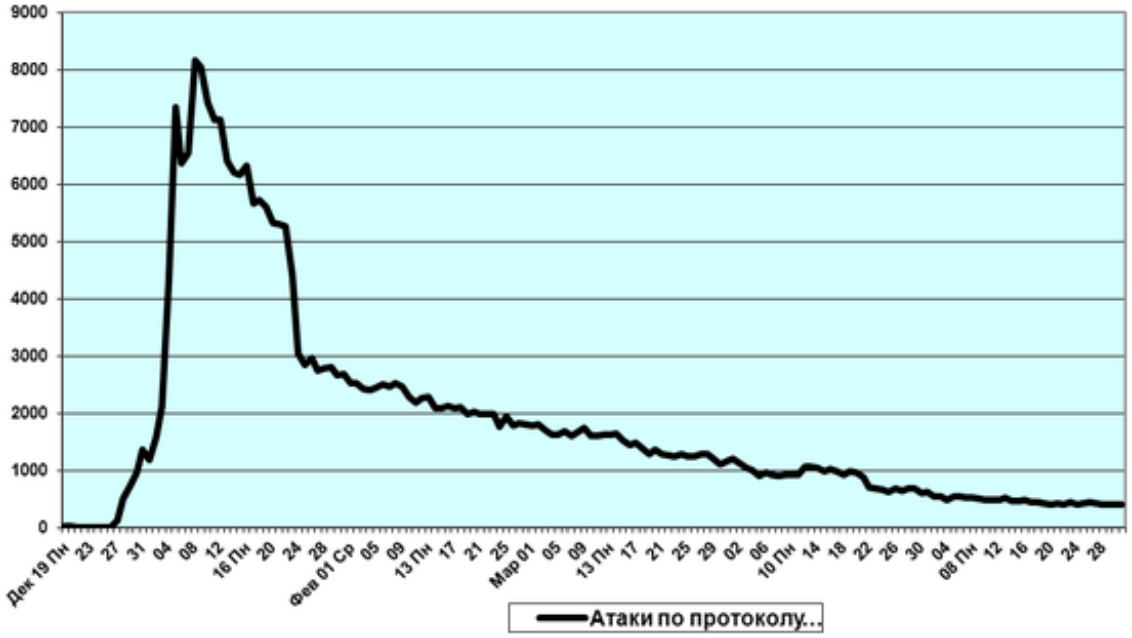

Рис.1. Объемы паразитного трафика GRE-пакетов (декабрь 2016-Май 2017).

15 В общих чертах эта диаграмма напоминает графическое отображениие концепции, называемой в теории маркетинга «Жизненный цикл товара»[8] [9]. В данном случае напрямую

зарегистрированый паразитный трафик соответствует не показателям «продажи товара» или «прибыль от реализации», а отражает непосредственное потребление приобретенного «товара» – использование средств организации атак на сети.

16 Этапы жизненного цикла данного «товара» представлены в полном соответствии с упомянутой концепцией :

- Разработка и внедрение - первые пробы 04- 08 августа, старт «продаж» - 19 декабря.
- Этап роста – 19-28 декабря, бурный рост -29 декабря-04 января,
- Этап зрелости – 05 - 24 января
- Этап упадка – постепенное снижение использования – 25 января -по настоящее время. С конца июля того же года использование можно считеть незначительным – около двухсот атак в сутки.

17 Столь кратковременная реализация жизненного цикла атаки (декабрь-январь 2016 г.) связана с особенностями сетевой среды Интернета:

- цель создания и использования средств атаки– нелегитимное проникновение в посторонние сети (в данном случае – в сеть ЦЭМИ РАН), поэтому каждая отдельная атака кратковременна;
- реализация, распространение и использование средств атаки происходит в сетевой среде Интернета, характерной высокой скоростью проведения электронных торговых операций и доставки приобретенного электронного товара;
- потребность в данном «товаре» активно подогревалась в СМИ (как раз в этот период проходили выборы в США) с тематикой российского вмешательства. Снижение использования «товара» на максимуме графика соответствует периодам снижения активности СМИ в данном вопросе.

18 Влияние СМИ иллюстрирует диаграмма начальной стадии нарастания паразитного трафика (рис.2, декабрь 2016г. - январь 2017г.) . Кроме данных об объемах сканирования сети за указанный период, на диаграмме в верхнем ряду отмечены общественно значимые события, которые возможно и привели к данной нелегитимной активности в Интернете.

19

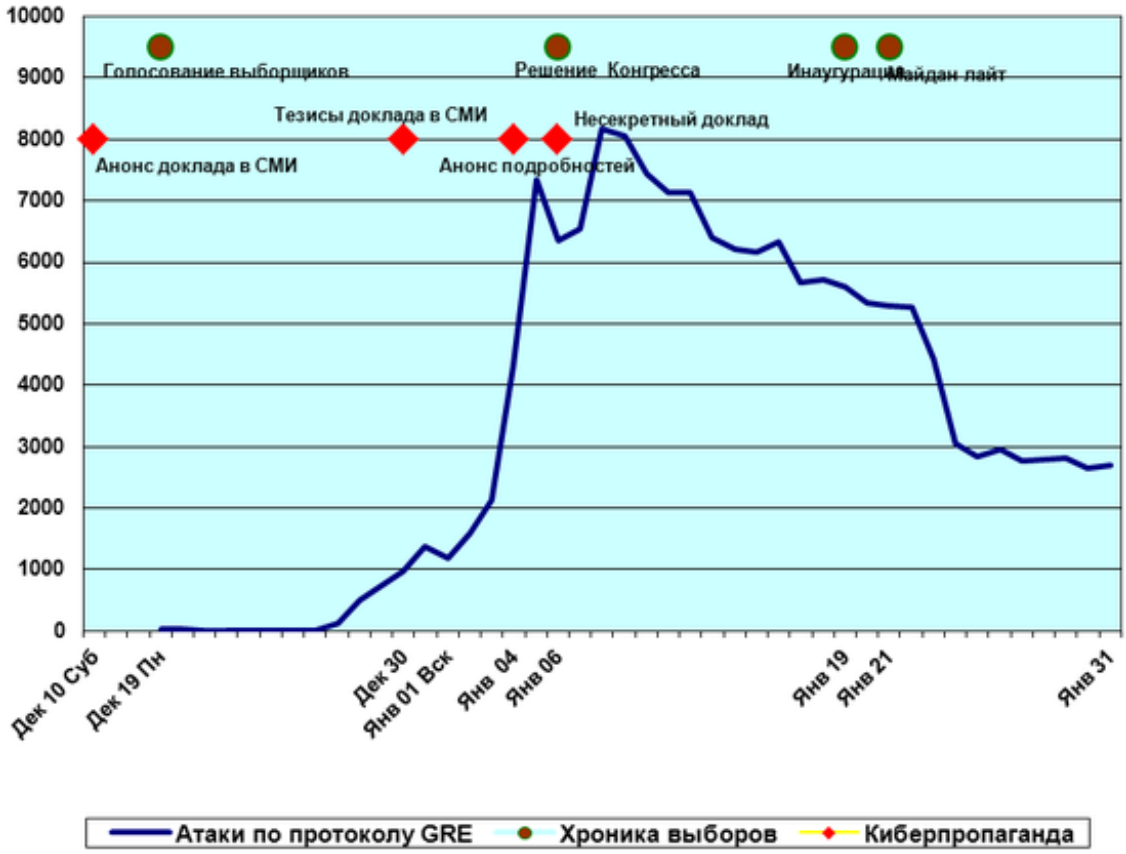

Рис.3. Рост паразитного трафика по протоколу GRE (декабрь 2016-январь 2017).

20 В верхнем ряду «Хроника выборов» отмечены некоторые вехи избирательной кампании в США, в течение которой в СМИ неоднократно возникали темы российского кибервмешательства в процесс выборов. Даты наиболее значимых моментов в обсуждении упомянутых тем отмечены во втором ряду – «Киберпропаганда». Датировка была взята из российских источников, поэтому имеется расхождение в датах процесса выборов и реакции графика в связи с разными часовыми поясами. Аналогично этому, датировка активности СМИ приводится из российских источников, с той же разницей часовых поясов анализируемой сети и массы пользователей интернета, реагирующей на нее. По мере снижения активности СМИ снижалась и активность пользователей средств организации атак на сети, однако полностьтю паразитный трафик не исчезает никогда.

21 **Постоянство паразитного трафика.** Во время написания статьи (май 2019 г.) было проведено небольшое исследование трафика GRE-пактов, чтобы определить, насколько он изменился за прошедшее время. Как оказалось, полностью этот трафик не исчез – это и есть постоянный уровень инфицированности интернет-среды, который достигается по мере потери интереса криминализированных пользователей к новооткрытым способам взлома сетей. Результат исследования (в течение недели) см. на рис.3 , разброс значений зависит от дня недели.

22

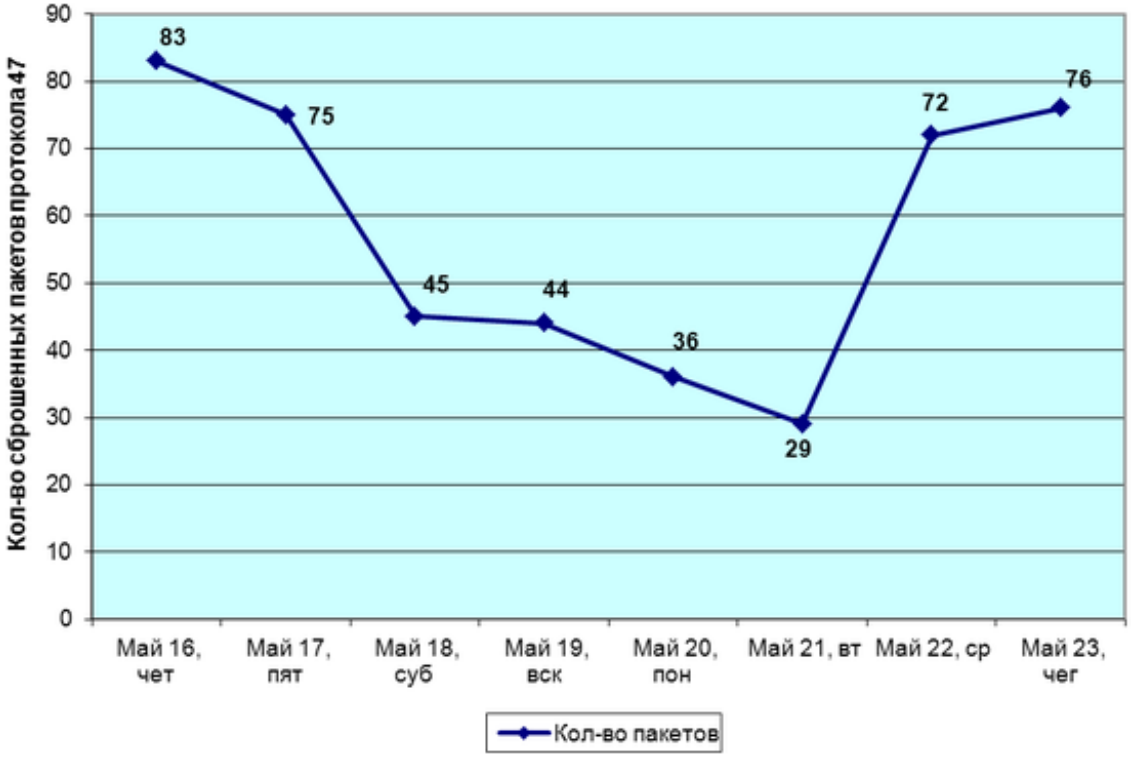

Рис.3. Объемы паразитного трафика GRE-пакетов за неделю 16-23.05.2019 г.

23 По сравнению с ранее достигнутым максимумом паразитного трафика GRE-пакетов (8000 пакетов в сутки) – постоянный его уровень незначителен. Текущий уровень паразитного трафика колеблется от ~80 до ~30 GRE-пакетов в день, что в среднем составляет 0,63 % от максимума. И он уже может считаться постоянным паразитным трафиком интернета, безуспешно пытающимся войти в сеть ЦЭМИ РАН.

24 Однако способов несанкционированного доступа множество, появление их происходит постоянно (так, только антивирусный продукт DrWeb имеет базу около миллиона вирусов, и она постоянно пополняется), так что суммарный уровень инфицированности потока данных из интернета (и соответственно загрузки сети паразитным трафиком) может достигать значительных величин.

25 **Выводы.** Первым выводом можно повторить всеобщую мысль о необходимости комплекса мер сетевой безопасности и антивирусной защиты сетевых ПК.

26 В качестве следующего вывода можно можно признать, что:

- сетевые продукты для нелегитимной деятельности давно являются интернет-товарами;
- так же, как другие товары, они обладают жизненным циклом, зависящим от их успеха в использовании и развернутой рекламы товара в сетевой среде;
- угасание интереса к использованию данных сетевых продуктов зависит от неуспеха их использования, который, в свою очередь, определяется качеством защиты сети от проникновения (причем новые «товары» желательно отвергать на стадии их первоначального внедрения).

27 Реализованная в ЦЭМИ РАН и постоянно поддерживаемая политика разрешительного доступа в сеть[10] [11] в сочетании с комплексом антивирусной защиты[12] [13] [14] позволяют успешно противодействовать предпринимаемым атакам на сеть института.

Примечания:

1. Ляпичева Н.Г. Информационные сервисы и обеспечение их защиты от несанкционированного доступа из Интернет. / В сб. “Использование и развитие современных информационных технологий в научных исследованиях". М. ЦЭМИ РАН 2003, с. 32 - 63, ISBN 5-8211-0262-6

2. Ляпичева Н.Г. Обнаружение сетевых почтовых атак. / "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 2". - Сб.статей под ред. М.Д.Ильменского. - М., ЦЭМИ РАН, 2005, с.28-39, ISBN 5-8211-0365-7. >>>>

3. Кочетова Н.А., Ляпичева Н.Г. Опыт использования сетевого экрана ASA5510 в качестве граничного маршрутизатора корпоративной сети / "Развитие технологий и инструментальных средств информационной безопасности. Выпуск 2". - Сб.статей под ред. А.М.Терентьева. - М., ЦЭМИ РАН, 2012, с.22-33, ISBN 978-5-8211-0615-5.

4. RFC 2784 - Generic Routing Encapsulation (GRE)>>>> [Электронный ресурс : 29 мая 2019 г.

5. PROTOCOL NUMBERS: / RFC 1700 - ASSIGNED NUMBERShttps://tools.ietf.org/html/rfc1700 [Электронный ресурс : 29 мая 2019 г.

6. Зайцев А.С. Туннели GRE между объектами /

7. Кочетова Н.А., Ляпичева Н.Г. Опыт использования сетевого экрана ASA5510 в качестве граничного маршрутизатора корпоративной сети / "Развитие технологий и инструментальных средств информационной безопасности. Выпуск 2". - Сб.статей под ред. А.М.Терентьева. - М., ЦЭМИ РАН, 2012, с.22-33, ISBN 978-5-8211-0615-5.

8. Жизненный цикл товара. Лекции по Маркетингу 1 [Электронный ресурс : 21 августа 2019 г.] >>>>

9. Сушко Д.Е. Моделирование кривых жизненного цикла товара. / ВЕСТНИК УНИВЕРСИТЕТА РОССИЙСКОЙ АКАДЕМИИ ОБРАЗОВАНИЯ. Университет РАО (Москва), 2010, №2 стр.128-130 ISSN: 2072-5833

10. Вопросы информационной безопасности узла Интернет в научных организациях / Сборник трудов под ред. М.Д.Ильменского. - М: ЦЭМИ РАН, 2001 - 73с. (Рус). ISBN 5-8211-0134-4

11. Кочетова Н.А.,Ляпичева Н.Г. Методы и средства защиты маршрутизаторов и серверов удаленного доступа производства Cisco Systems / В сб. под ред. Ильменского М.Д. Вопросы информационной безопасности узла Интернет в научных организациях. ЦЭМИ РАН, М. 2001. стр.10-42. ISBN 5-8211-0134-4

12. Терентьев А.М. Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях: монография / А.М.Терентьев. - Чебоксары. ИД "Среда", 2018. - 100 с. - ISBN 978-5-6040294-5-9, DOI 10/31483/в-15, DOI 10.31483/г-11245.

13. А.М.Терентьев. Выбор адекватных средств информационной защиты персонального компьютера в России // "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N33(174), 2012, с.37-42, ISSN 2073-2872

14. Терентьев А.М. Сетевой мониторинг. Методы и средства. Том 1: монография / А.М.Терентьев. - Чебоксары. ИД "Среда", 2019. - 116 с. - ISBN 978-5-6042304-9-7, DOI 10.31483/а-62.

Библиография:

1. Ляпичева Н.Г. Информационные сервисы и обеспечение их защиты от несанкционированного доступа из Интернет. / В сб. “Использование и развитие современных информационных технологий в научных исследованиях". М. ЦЭМИ РАН 2003, с. 32 - 63, ISBN 5-8211-0262-6

2. Ляпичева Н.Г. Обнаружение сетевых почтовых атак. / "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 2". - Сб.статей под ред. М.Д.Ильменского. - М., ЦЭМИ РАН, 2005, с.28-39, ISBN 5-8211-0365-7. http://av.cemi.rssi.ru/av/r4lit18.htm

3. Кочетова Н.А., Ляпичева Н.Г. Опыт использования сетевого экрана ASA5510 в качестве граничного маршрутизатора корпоративной сети / "Развитие технологий и инструментальных средств информационной безопасности. Выпуск 2". - Сб.статей под ред. А.М.Терентьева. - М.,

ЦЭМИ РАН, 2012, с.22-33, ISBN 978-5-8211-0615-5.

4. RFC 2784 - Generic Routing Encapsulation (GRE) https://tools.ietf.org/html/rfc2784 [Электронный ресурс : 29 мая 2019 г.]

5. PROTOCOL NUMBERS: / RFC 1700 - ASSIGNED NUMBERS https://tools.ietf.org/html/rfc1700 [Электронный ресурс : 29 мая 2019 г.]

6. Зайцев А.С. Туннели GRE между объектами / http://zaycev.me/index.php/myblog/entry/2015/12/18/tunneli-gre-mezhdu-ob-ektami [Электронный ресурс : 18 декабря 2015 г.]

7. Кочетова Н.А., Ляпичева Н.Г. Опыт использования сетевого экрана ASA5510 в качестве граничного маршрутизатора корпоративной сети / "Развитие технологий и инструментальных средств информационной безопасности. Выпуск 2". - Сб.статей под ред. А.М.Терентьева. - М., ЦЭМИ РАН, 2012, с.22-33, ISBN 978-5-8211-0615-5.

8. Жизненный цикл товара. Лекции по Маркетингу 1 http://www.grandars.ru/student/marketing/zhiznennyy-cikl-tovara.html [Электронный ресурс : 21 августа 2019 г.]

9. Сушко Д.Е. Моделирование кривых жизненного цикла товара. / ВЕСТНИК УНИВЕРСИТЕТА РОССИЙСКОЙ АКАДЕМИИ ОБРАЗОВАНИЯ. Университет РАО (Москва), 2010, №2 стр.128-130 ISSN: 2072-5833

10. Вопросы информационной безопасности узла Интернет в научных организациях / Сборник трудов под ред. М.Д.Ильменского. - М: ЦЭМИ РАН, 2001 - 73с. (Рус). ISBN 5-8211-0134-4

11. Кочетова Н.А., Ляпичева Н.Г. Методы и средства защиты маршрутизаторов и серверов удаленного доступа производства Cisco Systems / В сб. под ред. Ильменского М.Д. Вопросы информационной безопасности узла Интернет в научных организациях. ЦЭМИ РАН, М. 2001. стр.10-42. ISBN 5-8211-0134-4

12. Терентьев А.М. Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях: монография / А.М.Терентьев. - Чебоксары. ИД "Среда", 2018. - 100 с. - ISBN 978-5-6040294-5-9, DOI 10/31483/в-15, DOI 10.31483/г-11245.

13. Терентьев А.М.. Выбор адекватных средств информационной защиты персонального компьютера в России // "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N33(174), 2012, с.37-42, ISSN 2073-2872

14. Терентьев А.М. Сетевой мониторинг. Методы и средства. Том 1: монография / А.М.Терентьев. - Чебоксары. ИД "Среда", 2019. - 116 с. - ISBN 978-5-6042304-9-7, DOI 10.31483/а-62.

Parasitic traffic in Internet : lifecycle of the GRE packet attack

N. Lyapicheva
CEMI RAS
Moscow, Nakhimovsky prospect, 47

Abstract

The lifecycle of the network attack with GRE packets and its influense on Internet traffic is considered on the basis of the logging data. The role of the mass media on the increase and decline in the lifecycle of the attack is noted. The reasonability of prohibitive policy of access from the Internet is noted.

Keywords: computer networks, internet security, network scanning, security appliance, lifecycle of attack

Date of publication: 07.02.2020

Citation link:

Lyapicheva N. Parasitic traffic in Internet : lifecycle of the GRE packet attack // Herald of CEMI. 2019. Issue 3 [Electronic resource]. Access for registered users. URL: https://cemi.jes.su/s265838870007146-3-1/ (circulation date: 10.02.2020). DOI: 10.33276/S265838870007146-3

Код пользователя: 7792; Дата выгрузки: 10.02.2020; URL - http://cemi.jes.su/s265838870007146-3-1/ Все права защищены.