ВЫХОДНЫЕ ДАННЫЕ ЖУРНАЛА

https://www.elibrary.ru/item.asp?id=43827539
http://old.imi-samara.ru/node/103
https://www.elibrary.ru/download/elibrary_43827539_89555795.pdf

Журнал РИНЦ /ВАК по естественно-научным и техническим направлениям

РИНЦ- да
Офилирована с ВГУЭС

Импакт фактор 0,464

НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU

КОРЗИНА

ПОИСК

НАВИГАТОР

СЕССИЯ

ИНФОРМАЦИЯ О ПУБЛИКАЦИИ

eLIBRARY ID: 43827539

ВРЕДОНОСНЫЕ ПРОГРАММЫ В КОМПЬЮТЕРНЫХ СЕТЯХ: DDOS-АТАКИ И ИХ ПОСЛЕДСТВИЯ

ВАСИЛЕНКО К.А.[1], ЗОЛКИН А.Л.[2], АБРАМОВ Н.В.[3], КУРГАНОВ Д.О.[3]

[1] Владивостокский государственный университет экономики и сервиса, г.Владивосток, Россия
[2] Средневолжская специализированная производственная база, г. Самара, Россия
[3] Дальневосточный федеральный университет, г.Владивосток, Россия

Тип: статья в журнале - научная статья Язык: русский

Номер: 2 Год: 2020 Страницы: 108-111

УДК: 004.056

ЖУРНАЛ:

ВЕСТНИК МЕЖДУНАРОДНОГО ИНСТИТУТА РЫНКА
Учредители: Международный институт рынка (Самара)

КЛЮЧЕВЫЕ СЛОВА:

КОМПЬЮТЕРНЫЕ СЕТИ, WEB-СЕРВЕР, ВРЕДОНОСНЫЕ ПРОГРАММЫ, DDOS-АТАКИ, ИНФОРМАЦИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, COMPUTER NETWORKS, WEB SERVER, MALICIOUS SOFTWARE, DDOS ATTACKS, INFORMATION, CYBER SECURITY

АННОТАЦИЯ:

Настоящая статья посвящена исследованию проблем, связанных с угрозой, исходящей от вредоносных программ в компьютерных сетях, таких как непосредственно DDOS-атаки; выявлены особенности таких программ, а также приведены способы, позволяющие с ними бороться. Следует констатировать, что всемирная сеть Интернет сегодня уже не рассматривается как полноценное безопасное информационное поле для пользователей. Связано это прежде всего с тем, что современные антивирусные программы в отношении скорости отстают по модернизации и не «успевают» за развитием новых вредоносных программ, атак и взломов, несмотря на постоянное обновление защитной базы. В настоящий момент непосредственно рабочая станция обычного пользователя используется злоумышленником в собственных интересах с целью атаковать более крупную информационную «кибер-жертву». Необходимо, чтобы защитный способ от вредоносных программных атак заблаговременно уже на стадии его разработки создавался с учетом указанных обстоятельств.

БИБЛИОМЕТРИЧЕСКИЕ ПОКАЗАТЕЛИ:

Входит в РИНЦ®: да	Цитирований в РИНЦ®: 0
Входит в ядро РИНЦ®: нет	Цитирований из ядра РИНЦ®: 0
Входит в Scopus®:	Цитирований в Scopus®:
Входит в Web of Science®:	Цитирований в Web of Science®:
Норм. цитируемость по журналу:	Импакт-фактор журнала в РИНЦ:
Норм. цитируемость по направлению:	Дециль в рейтинге по направлению:

Тематическое направление: Social and economic geography

ПОКАЗАТЕЛИ ПО ГОДАМ

Название показателя	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Число статей в РИНЦ	0	0	0	0	0	59	57	50	47	51
Число выпусков журнала в РИНЦ	0	0	0	0	0	2	2	2	2	2
Показатель журнала в рейтинге SCIENCE INDEX	-	-	-	-	-	0,000	0,013	0,027	0,022	0,026
Место журнала в рейтинге SCIENCE INDEX	-	-	-	-	-	3638	3508	3429	3663	3552
Двухлетний импакт-фактор РИНЦ	-	-	-	-	-	-	-	0,784	0,364	0,464
Двухлетний импакт-фактор РИНЦ с учетом цитирования из всех источников	-	-	-	-	-	-	-	0,862	0,477	0,660

ИНФОРМАЦИЯ О ЖУРНАЛЕ

Полное название	ВЕСТНИК МЕЖДУНАРОДНОГО ИНСТИТУТА РЫНКА		
Издательство	Частное образовательное учреждение высшего образования "Международный институт рынка"		
Год основания	2006	Рецензируемый	
Выпусков в год	2	Импакт-фактор JCR	нет

Возможные действия

- Просмотреть оглавления выпусков журнала
- Искать статьи в этом журнале
- Вывести список статей, опубликованных в данном журнале
- Вывести список публикаций, ссылающихся на статьи в данном журнале

Сокращение		Страна	Россия
Город	Самара	Регион	Самарская область

Печатная версия журнала

ISSN печатной версии		Подписной индекс		Тираж	

Электронная онлайновая версия журнала

ISSN онлайновой версии		Вариант представления	
WWW-адрес	http://old.imi-samara.ru/node/103		

ISI	нет	Всего статей	334	В настоящее время	выходит
SCOPUS	нет	Всего выпусков	15	Доступный архив	2006 - 2020
РИНЦ	да	Полных текстов	326	Реферативный	нет
Перечень ВАК		Цитирований	705	Мультидисциплинарный	да
RSCI	нет	DOAJ	нет		

РАЗДЕЛ V. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

ВРЕДОНОСНЫЕ ПРОГРАММЫ В КОМПЬЮТЕРНЫХ СЕТЯХ: DDOS-АТАКИ И ИХ ПОСЛЕДСТВИЯ

© 2020 Василенко К.А.[1], Золкин А.Л.[2], Абрамов Н.В.[3], Курганов Д.О.[3]

[1]Владивостокский государственный университет экономики и сервиса, г.Владивосток, Россия
[2]Средневолжская специализированная производственная база, г. Самара, Россия
[3]Дальневосточный федеральный университет, г.Владивосток, Россия

Настоящая статья посвящена исследованию проблем, связанных с угрозой, исходящей от вредоносных программ в компьютерных сетях, таких как непосредственно DDOS-атаки; выявлены особенности таких программ, а также приведены способы, позволяющие с ними бороться. Следует констатировать, что всемирная сеть Интернет сегодня уже не рассматривается как полноценное безопасное информационное поле для пользователей. Связано это прежде всего с тем, что современные антивирусные программы в отношении скорости отстают по модернизации и не «успевают» за развитием новых вредоносных программ, атак и взломов, несмотря на постоянное обновление защитной базы. В настоящий момент непосредственно рабочая станция обычного пользователя используется злоумышленником в собственных интересах с целью атаковать более крупную информационную «кибержертву». Необходимо, чтобы защитный способ от вредоносных программных атак заблаговременно уже на стадии его разработки создавался с учетом указанных обстоятельств.

Ключевые слова: компьютерные сети, web-сервер, вредоносные программы, DDOS-атаки, информация, информационная безопасность.

На современном этапе развития рынка услуг по защите информации все большую актуальность приобретает проблема защиты WEB-сервера от так называемых DDOS-атак. В переводе с английского DDOS (Distributed Denial of Service) означает распределенный отказ в обслуживании. «Такой» способ атаки имеет своей целью вывод из штатного рабочего состояния атакуемую вычислительную машину. Как правило, данный вид атаки применяется в качестве инструмента для шантажа, ликвидаем этого скрипта на посещаемой странице какого-нибудь WEB-сайта [10].

Если данный ресурс отсутствует, то злоумышленник очень просто сделает фейковый сайт и осуществит спам-рассылку, содержащую ссылку на страницу с вредоносным кодом. В итоге из-за скопления пользователей создастся множество запросов, от которых сервер оказывается просто перегружен при попытке их обработки [2, 3].

Приведенный выше пример демонстрирует

****