УДК 056+002:004.056

ОПРЕДЕЛЕНИЕ АТРИБУТОВ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С АКТИВНОСТЬЮ ИНТЕРНЕТ-БОТОВ

Логинова А.О.

Московский государственный лингвистический университет, г. Москва, Российская Федерация

Научный руководитель: Царегородцев А.В. – д-р техн.наук, профессор, профессор кафедры международной информационной безопасности Института информационных наук ФГБОУ ВО МГЛУ, проректор по развитию и информатизации ФГБОУ ВО МГЛУ

Аннотация. Исследовано воздействие ботов на работоспособность Интернет-средств массовой коммуникации. Для автоматизированного управления событиями, предупреждающими отказ в обслуживании, блокировку Интернет-средств массовой информации за нарушение законодательства, в результате действий злонамеренных ботов, были определены атрибуты классификации, установлены возможные значения атрибутов событий, предупреждающих инциденты, связанные с активностью Интернет-ботов.

Ключевые слова: события информационной безопасности, атрибуты событий информационной безопасности, Интернет-боты, Интернет-средства массовой коммуникации.

Введение. Стремительное развитие информационно-коммуникационных технологий (ИКТ), доступность средств сбора, обработки, хранения и распространения информации, а также отсутствие границ информационного обмена обуславливают интенсивность развития и распространения Интернет-средств массовой коммуникации (Интернет-СМК): блогов, форумов, мессенджеров, социальных сетей, – что приводит к росту объёма различного рода информации, провоцируя рост информационных потребностей человека.

В условиях, когда средства ведения компьютерной атаки есть в каждой квартире, каждом офисе и каждом кабинете, скорость обнаружения опасного события информационной безопасности (ИБ) приобретает важное значение.

Согласно результатам исследования *GlobalDots*, опубликованным в 2019 году, 37,9% Интернет-трафика в 2018 году создавали боты. При этом большинство действующих ботов были высокоорганизованными: боты с применением технологии искусственного интеллекта, способные копировать поведение человека, они составили 21,1% от обнаруженного множества ботов, и управляемые боты – 52,5%. По данным аналитиков *GlobalDots* в период с 2013 года по 2019 год в сети было украдено свыше 14 миллиардов персональных аккаунтов реальных пользователей. С помощью ботов злоумышленники проверяют пригодность украденной учетной записи для её дальнейшего использования ботом [1].

Основная часть. При реализации атаки любого типа нарушитель выполняет определённую последовательность шагов (рисунок 1).

Рисунок 1 – Жизненный цикл атаки

Ранее в работах были подробно описаны основные группы событий ИБ [2, 3]. При ближайшем рассмотрении самих инцидентов сбора информации, несанкционированного доступа, внедрения вредоносного кода можно проследить их взаимосвязь. Они представляют собой этапы развития *DoS*/*DDoS* атаки (рисунок 2).

Рисунок 2 – Этапы развития *DoS/DDoS* атаки

По принципу реализации атака посредством «наводнения» Интернет-источников информации сообщениями ботов представляет собой частный случай *DoS*/*DDoS* атаки. Скрывая свою природу, боты распространяют спам и ложную информацию. Способность делать информационные вбросы, выдавать мнение меньшинства за позицию большинства, искажая восприятие человеком реальных событий [4], делает ботов одним из барьеров в формировании корректного новостного фона, смещая смысловые и идеологические акценты и тем самым создавая угрозы киберустойчивости и цифрового суверенитета государства [5].

Конечно, *DoS*/*DDoS* атака может и не представлять саму цель злоумышленника. Суть этой цепи заключается в том, что все события, возникающие по пути реализации этой атаки, будут повторять ряд уже известных нам событий, связанных со сбором информации о сети, несанкционированным доступом и внедрением вредоносного кода, это значит, что и атрибуты будут общими.

Все атрибуты событий могут быть получены в результате наблюдения и анализа процессов в системе. Таким образом, можно получить значение каждого атрибута при разных обстоятельствах. Для экономии времени специалисты договорились использовать атрибуты, установленные в базах *KDD-Cup*'99, *NSL-KDD* и *Kyoto* 2006+.

Приведём сравнительную таблицу вышеупомянутых баз атрибутов событий ИБ (таблица 1).

Таблица 1 – Сравнение баз атрибутов *KDD-Cup*'99, *NSL-KDD* и *Kyoto* 2006+

База атрибутов	**Количество атрибутов**	**Достоинства**	**Недостатки**
KDD-Cup'99 (1999г.)	41 (из 1998 *DARPA*)	– используется в системах оценки аномалий; – тип атаки в тренировочном варианте отличался от тестового	– содержит избыточные записи; – устарела
NSL-KDD (2009г.)	41 (из *KDD-Cup*'99)	– не содержит избыточных записей; – число записей обосновано	– не адаптирована под работу реальной сети
Kyoto 2006+ (2009г.)	24 (14 из *KDD-Cup*'99 + 10 дополнительных)	– игнорируются избыточные атрибуты; – представляется реально существующая сеть	– не содержит информации о реализуемом типе атаки

Для решения задачи классификации событий ИБ возьмём атрибуты, описанные в базе данных *Kyoto* 2006+, поскольку представленные в ней атрибуты событий ИБ были выделены при анализе трафика реальной сетьи. Компоненты базы *Kyoto* 2006+ повторяют признаки опасных событий сбора информации о сети.

Для наглядности будем возьмём 24 атрибута базы *Kyoto* 2006+, комбинации которых будут отражать реализацию атаки. (таблица 2).

Таблица 2 – Атрибуты *Kyoto* 2006+

№ п/п	Атрибут	Описание
1.	*Duration1*	продолжительность соединения
2.	*Service*	тип сервера подключения
3.	*Source bytes*	количество байт информации, переданное с *IP* отправителя
4.	*Destination bytes*	количество байт информации, переданное с *IP* получателя
5.	*Count*	количество соединений, где *IP* отправителя и *IP* получателя идентичны *IP* адресам текущего соединения в течение последних 2-х секунд
6.	*Same_srv_rate*	% соединений от одного и того же сервера
7.	*Serror_rate*	% соединений с ошибками *SYN*
8.	*Srv_serror_rate*	% соединений с ошибками *SYN* в *Srv_count* (% соединений, где тип сервиса идентичен типу сервиса текущего соединения в течение последних 2-х секунд)
9.	*Dst_host_count*	количество соединений среди последних 100, где *IP* получателя одинаковы *IP* адресам текущего соединения; количество соединений, где *IP* источника также идентичен адресу текущего соединения
10.	*Dst_host_srv_count*	количество соединений среди последних 100, где *IP* получателя одинаковы *IP* адресам текущего соединения; тип сервиса идентичен типу сервиса текущего соединения;
11.	*Dst_host_same_scr_port_rate*	% соединений, где порт-отправитель идентичен порту текущего соединения в *Dst_host_count*
12.	*Dst_host_serror_rate*	% соединений с ошибками *SYN* в *Dst_host_count*
13.	*Dst_host_srv_serror_rate*	% соединений с ошибками *SYN* в *Dst_host_srv_count*
14.	*Flag*	состояние соединения в момент записи соединения
15.	*IDS_detection*	индикатор срабатывания системы обнаружения вторжений: 0 - нет срабатываний; целые числе (без учёта значения «0») - количество срабатываний
16.	*Malware_detection*	индикатор вредоносного кода: 0 - нет вредоносного кода; текстовая строка - обозначение передаваемого при соединении вредоносного кода
17.	*Ashula_detection*	индикатор использования шелл-кода (исполняемый код, передаёт управление процессору) или эксплоит-кода при соединении: 0 -нет кода; целые числе (без учёта значения «0») - количество различных передаваемых кодов
18.	*Label*	индикатор наличия атаки сессии: 1 - нормальное функционирование; -1 - известный тип атаки в сессии; -2 - неизвестный тип атаки в сессии
19.	*Source_IP_Address*	обозначает *IP* отправителя, используемый в сессии. Одинаковые частные *IP* адреса действительны только в течение одного месяца, это означает, что их *IP* адреса *IPv*4 были также одинаковыми; но, если 2 частных *IP* адреса одинаковы в контексте разных месяцев, то их IP адреса *IPv*4 были различны
20.	*Source_Porte_Number*	индикатор номера порта отправителя, используемый в сессии
21.	*Destination_IP_Address*	обозначает *IP* получателя, используемый в сессии (аналогично пункту 19)
22.	*Destination_Port_Number*	индикатор номера порта получателя, используемый в сессии
23.	*Start_Time*	индикатор начала сессии
24.	*Duration2*	индикатор сессии, отображающий время, за которое устанавливалась сессия

Во избежание ложных срабатываний системы обнаружения событий ИБ установим только 2 значения для каждого из атрибутов: «меньше порогового» (доверительный интервал) и «больше или равно пороговому» (интервал «опасных» значений).

Поскольку всё множество значений было взято из результатов мониторинга проводимых атак *Kyoto*2006+, в которых не было определено, при каком конкретном значении атрибута было зафиксировано начало атаки, в каждом столбце указали примерные доверительные интервалы значений атрибутов, т.е. предположили, в каких интервалах значений атрибутов не фиксировался инцидент. Так фасетная классификация атрибутов событий информационной безопасности будет иметь следующий вид (таблица 3).

Таблица 3 – Фасетная классификация атрибутов событий ИБ

№ п/п	Атрибут/фасет	Возможные значения	
		доверительный интервал	интервал опасных значений
1.	*Duration1*	(1; 10)	[0,000000; 1] U [10; +∞)
2.	*Source bytes*	[0; 1000)	[1000; +∞)
3.	*Destination bytes*	[0; 1000)	[1000; +∞)
4.	*Count*	[0; 1)	[1; +∞)
5.	*Same_srv_rate*	[0; 1)	[1; 100]
6.	*Serror_rate*	[0; 1)	[1; 100]
7.	*Srv_serror_rate*	[0; 1)	[1; 100]
8.	*Dst_host_count*	[0; 1)	[1; 100]
9.	*Dst_host_srv_count*	[0; 5)	[5; 100]
10.	*Dst_host_same_scr_port_rate*	[0; 0,01)	[0,01; 100]
11.	*Dst_host_serror_rate*	[0; 0,10)	[0,10; 100]
12.	*Dst_host_srv_serror_rate*	[0; 0,01)	[0,01; 100]
13.	*IDS_detection*	0	(0;+*Z*), где *Z*-целые числа
14.	*Malware_detection*	0	строка кода
15.	*Ashula_detection*	0	(0;+*Z*)
16.	*Label*	1	-1, -2
17.	Service	*dns*, *http*, *smtp*, *ssh*, *ssl*, *other*	
18.	Flag	*OTH*, *REJ*, *RSTO*, *RSTOS0*, *RSTR*, *RSTRH*, *S0*, *SF*, *SH*, *SHR*	
19.	Source_IP_Address	*IP*-адрес	…
20.	Source_Porte_Number	номер порта	…
21.	Destination_IP_Address	IP-адрес	…
22.	Destination_Port_Number	номер порта	…
23.	Start_Time	время начала сессии	…
24.	Duration2	длительность сессии	…

Стоит заметить, что при необходимости можно дополнить таблицу новыми атрибутами и их значениями, а также изменить значения интервалов.

Определим набор атрибутов события ИБ, по которым то или иное событие можно будет однозначно отнести к конкретной группе событий, предшествующих инциденту (таблица 4).

Таблица 4 – Наборы атрибутов для каждой группы событий ИБ

№ п/п	Группа	Набор атрибутов
1.	События сбора информации о сети	− *Service;* − *Destination bytes;* − *Count;* − *Same_srv_rate;* − *Serror_rate;* − *Srv_serror_rate;* − *Dst_host_count;* − *Dst_host_srv_count;* − *Dst_host_same_scr_port_rate;* − *Dst_host_serror_rate;* − *Dst_host_srv_serror_rate;* − *Flag;* − *Source_IP_Address;* − *Source_Porte_Number;* − *Destination_IP_Address;* − *Destination_Port_Number;* − *Duration2*
2.	События НСД	− *Source bytes;* − *Destination bytes;* − *Same_srv_rate;* − *Dst_host_same_scr_port_rate;* − *Flag;* − *IDS_detection;* − *Malware_detection;* − *Ashula_detection;* − *Label;* − *Source_IP_Address;* − *Start_Time;* − *Duration2*
3.	События внедрения вредоносного кода	− *Duration1;* − *Source bytes;* − *Dst_host_same_scr_port_rate;* − *Flag;* − *IDS_detection;* − *IDS_detection;* − *Malware_detection;* − *Destination_Port_Number;* − *Start_Time;* − *Duration2*

Как отмечалось ранее, события, являющиеся проявлением инцидентов сбора информации, несанкционированного доступа, внедрения вредоносного кода представляют собой части жизненного цикла *DoS*/*DDoS* атаки, а в частности инцидентов ИБ, связанных с активностью Интернет-ботов. Поэтому набор атрибутов для отслеживания такого типа атаки включает в себя атрибуты всех вышестоящих событий (таблица 5).

Таблица 5 – Набор атрибутов событий, предупреждающих инциденты, связанные с активностью Интернет-ботов

События отказа в обслуживании	– *Duration1;* – *Service;* – *Source bytes;* – *Count;* – *Same_srv_rate;* – *Serror_rate;* – *Srv_serror_rate;* – *Dst_host_count;* – *Dst_host_srv_count;* – *Dst_host_same_scr_port_rate;*	– *Dst_host_serror_rate;* – *Dst_host_srv_serror_rate;* – *Flag;* – *Label;* – *Source_IP_Address;* – *Source_Porte_Number;* – *Destination_IP_Address;* – *Destination_Port_Number;* – *Start_Time*

Набор атрибутов можно изменить (расширить или сократить) под условия поставленной задачи поиска события ИБ.

Заключение. Такая концепция представления множества возникающих в АИС событий ИБ в машиночитаемом виде, может использоваться для обнаружения признаков реализации частного случая *DoS*/*DDoS* атаки – «наводнения» Интернет-средств массовой коммуникации сообщениями ботов.

Для автоматизированного управления событиями, предупреждающими отказ в обслуживании, в частном случае блокировки Интернет-средств массовой информации за нарушение законодательства, в результате действий злонамеренных ботов, были определены атрибуты классификации событий ИБ, предупреждающих развитие инцидента отказа в обслуживании, установлены возможные значения атрибутов событий.

Список литературы

1. *Industry Report: Bad Bot Landscape 2019 // GlobalDots. We Make IT Faster URL:https://www.globaldots.com/bad-bot-report-2019#form (дата обращения: 15.12.2020).*

2 *Логинова, А.О. Типология множества событий информационной безопасности // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства. материалы XII Международной научно-практической конференции студентов, аспирантов и молодых ученых. - М.: Московский государственный лингвистический университет, 2021. - С. 69-74.*

3. *Логинова, А.О. Классификация существующих методов выявления инцидентов информационной безопасности / А.О. Логинова // Информационные технологии в науке, бизнесе и образовании: сб. тр. IX Международной науч.-практ. конф. студентов, аспирантов и молодых ученых. - Москва: ФГБОУ ВО МГЛУ, 2017. - С. 40-44.*

4. *Расторгуев С.П. Информационная война. – М.: Радио и связь, 1998. – 123 с.*

5. *Loginova, A.O., Aleynikova, D.V. Class allocation of events in an automated information system as the basis for increasing organization's cyber resilience /The Strategies of Modern Science Development: Proccedings of the XXI International scientific-practical conference, October 12-13, 2021, Morrisville, NC, USA, Section "Engineering". Lulu Press, Morrisville, NC, USA.*

UDC 056+002:004.056

DEFINING INFORMATION SECURITY EVENTS ATTRIBUTES RELATED TO THE ACTIVITY OF INTERNET BOTS

Loginova A.O.

Moscow state linguistic university, Moscow, The Russian Federation

Tsaregorodtsev A.V. – Dr. Tech. Sc., professor, professor of the Department of Information Security, Vice-rector for Development and Informatization of Moscow State Linguistic University

Annotation. It was examined the impact produced by bots on a performance of Internet mass media. There were defined attributes to classify information security events, possible values of information security event attributes related to bots' acts. The results could be applied to manage information security events taking place on forums, social networks, etc.

Keywords. information security events, information security events attributes, Internet bots, Internet mass media.