ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

старший лейтенант
Кобяков
Николай Сергеевич

Алгоритм применения мультипликаторов в регрессионном анализе для исследования деструктивных воздействий на АССН

АКТУАЛЬНОСТЬ

1.Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»
2.Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
3.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)
4.Руководство по организации процесса управления уязвимостями в органе (организации)
5.Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

АЛГОРИТМ ФОРМИРОВАНИЯ МОДЕЛИ

1. Определение пар поведенческих паттернов.
2. Определение мультипликаторов.
3. Формирование регрессионной модели с мультипликаторами.
4. Верификация полученной модели.

ПОВЕДНЧЕСКИЕ ПАТТЕРНЫ ВРЕДОНОСНЫХ УТИЛИТ

Наименование поведенческого паттерна	Обозначение
Проникновение на компьютер-жертву	p_1
Скрытие следов присутствия преступников в системе	p_2
Внесение в список разрешенных посетителей системы новых пользователей	p_3
Прекращение работы системы	p_4
Проведение атак типа «Отказ в обслуживании»	p_5
Сбор и анализ сетевых пакетов	p_6
Подмена адреса отправителя письма по электронной почте	p_7
Создание вредоносных программ	p_8
Навязывание ложной информации (уведомление об опасности, нарушениях)	p_9
Модификация вредоносных программ	p_{10}
Распространение флуда (бесполезных сообщений по каналам электронной почты)	p_{11}

ПАРЫ ПОВЕДНЧЕСКИХ ПАТТЕРНОВ И МУЛЬТИПЛИКАТОРЫ

$P_{4,5} = p_4 * p_5$
$P_{8,10} = p_8 * p_{10}$
$P_{7,11} = p_7 * p_{11}$

В/У	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p4*p5	p7*p11	p8*p10	J
1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	10
2	0	1	0	0	0	0	0	1	0	1	0	0	0	1	5,6
3	0	0	0	0	0	0	1	0	0	0	1	0	1	0	3,57
4	0	0	0	0	1	1	0	0	0	0	0	0	0	0	2,98
5	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1,78
6	0	0	0	1	1	1	0	0	0	0	0	1	0	0	9,2

ЛИНГВИСТИЧЕСКАЯ ШКАЛА

низкий [0.1-3.9]
средний [4.0 – 6.9]
высокий [7.0-8.9]
критический [9.0-10]

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

МОДЕЛЬ ДЛЯ ОЦЕНКИ ОПАСНОСТИ ВРЕДОНОСНЫХ УТИЛИТ

$$J = 0{,}453 + 4{,}855 * p_1 + 3{,}819 * p_2 + 1{,}415 * p_3 + 1{,}7 * p_4 + 0{,}875 * p_5 + 1{,}561 * p_6 + 0{,}833 * p_7 + 1 * p_8 + 0{,}78 * p_9 + 0{,}71 * p_{10} - 0{,}62 * p_{11} + 4{,}63 * p_{4*5} + 2{,}52 * p_{7*11} - 0{,}38 * p_{8*10}$$

ВЕРИФИКАЦИЯ МОДЕЛИ

№ п/п	Название	Паттерны	Опасность в результате опроса	Опасность с использование модели
1.	Constructor.DarkHorse	p_1, p_2, p_8, p_{10}	10	10,45
2.	Spy-Net 0.9	p_1, p_2	8,51	9,12
3.	DDoS.Siggen.41	p_4, p_5, p_{10}	8	8,36
4.	Linux.Siggen.5542	p_1, p_6	6,49	6,86
5.	Tool.TermService	p_3, p_7, p_{11}	5,91	4,6
6.	Linux.Siggen.322	p_1	5	5,31
7.	Tool.UDPFlood	p_3, p_{11}	2,64	1,25
8.	Tool.InstallToolbar.5	p_6, p_9	2,02	2,8
9.	Tool.Wpakill.4	p_7, p_9	2,02	2,07
10.	Tool.Spamer.18	p_9, p_{11}	0,813	0,62

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

1. Определение пар паттернов для других классов вредоносных программ.
2. Определение мультипликаторов для других классов вредоносных программ.
3. Формирование модели для оценки опасности деструктивных воздействий вредоносных программ.

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

старший лейтенант
Кобяков
Николай Сергеевич

Алгоритм применения мультипликаторов в регрессионном анализе для исследования деструктивных воздействий на АССН