«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ им. проф. М.А. БОНЧ - БРУЕВИЧА»

Подход к обнаружению аномалий и атак в Linux-системах на основе логов, полученных с использованием зонда eBPF

Докладчик: Виткова Л.А., ктн,
старший преподаватель, кафедра Защищенных систем связи
Соавтор исследования: М.В. Коломеец
Научный руководитель проекта: А.А. Чечулин

Актуальность

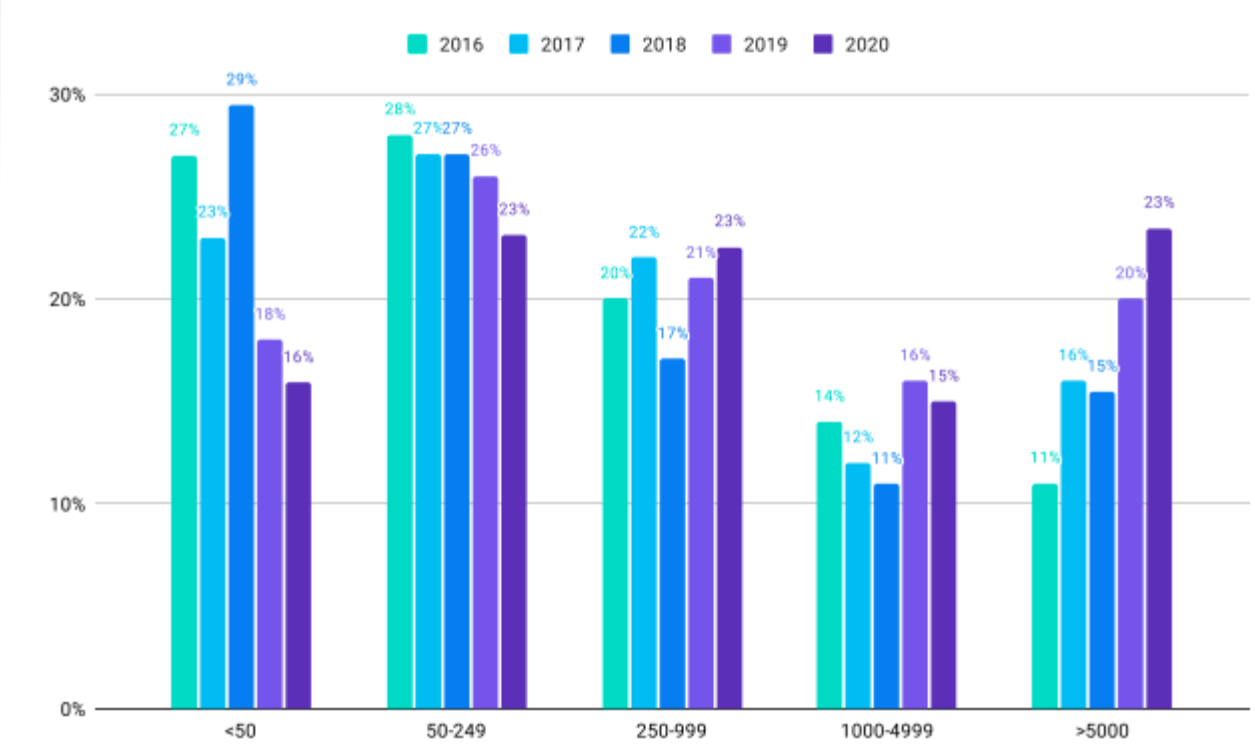

Диаграмма ответов на вопрос: «Сколько контейнеров обычно работает в вашей компании /организации?»*

- По данным Фонда облачных вычислений, использование контейнеров в производстве увеличилось на 300% в период с 2016 по 2020 год*

*По данным Фонда облачных вычислений, 2020г.

Актуальность

Диаграмма ответов на вопрос:
«Каковы ваши проблемы при использовании / развертывании контейнеров?»*

- В 2020 году проблема безопасности заняла третье место среди основных проблем использования контейнеров.*
- В 2021 году Контейнеры стали стандартом для доставки приложений и единицей для доставки вычислительных ресурсов и вспомогательных средств в эпоху облачных вычислений.**

* По данным Фонда облачных вычислений, 2020г.
** По данным Alibaba Cloud Container Service.

Безопасность контейнеров

Ключевые функции безопасности контейнера*

- Сканирование образов.
- Безопасность во время выполнения.
- Обнаружение угроз/сканирование уязвимостей.
- Сетевая безопасность.
- Реагирование на инциденты.
- Интеграция с инструментами DevOps и SIEM.

Популярные вендоры по информационной безопасности контейнеров*

- Sysdig (использует зонд eBPF)
- NeuVector.
- Alert Logic.
- Capsule8.
- Palo Alto Networks Prisma Cloud.
- Aqua Security (использует зонд eBPF).
- Anchore.

Основные подходы – анализ событий и журналов Linux

Только 2 вендора из списка популярных используют eBPF для сбора данных о событиях ядра в Linux.

* По данным eSecurity Planet, 2022

Признаки аномалий и атак

Признаки аномалии

1. Появление новых типов событий.
2. Исчезновение существующих типов событий.
3. Изменение интенсивности событий (количество в секунду).
4. Изменение пропорций типов событий.

Признаки атаки

1. Появление характерных типов событий.
2. Появление характерных аргументов событий.
3. Появление характерных последовательностей событий.

{"timestamp":1642241623416796410,"processId":1,"threadId":1,"parentProcessId":7161,"hostProcessId":7199,"hostThreadId":7199,"hostParentProcessId":7161,"userId":999,"mountNamespace":4026532268,"pidNamespace":4026532271,"processName":"redis-server",
"hostName":"5d5cafff8d25","containerId":"5d5cafff8d2512297c6e3d2312d4bd702c5c8445752e18adce70c4ecfd7fa900","eventId":"1018","eventName":"security_file_open","argsNum":5,"returnValue":0,"stackAddresses":null,"args":[{"name":"pathname","type":"const char*","value":"/proc/1/stat"},{"name":"flags","type":"int","value":32768},{"name":"dev","type":"dev_t","value":58},{"name":"inode","type":"unsigned long","value":30533},{"name":"ctime","type":"unsigned long","value":1642231042319992864}]}

Комплексный подход обнаружения аномалий и атак

Белые списки событий контейнера

Наблюдение за нормальной активностью контейнера, формирование белых списков:

a. системных вызовов;
b. системных вызовов и их аргументов;
c. последовательности системных вызовов.

Черные списки событий контейнера

Наблюдение за аномальной активностью контейнера (атакой) , формирование черных списков:

a. системных вызовов;
b. системных вызовов и их аргументов;
c. последовательности системных вызовов.

Тестирование подходов обнаружения

dataset	container	list_type	APPR_1_TP	APPR_1_TN	APPR_1_FP	APPR_1_FN	APPR_2_TP	APPR_2_TN	APPR_2_FP	APPR_2_FN	APPR_3_TP	APPR_3_TN	APPR_3_FP	APPR_3_FN
16	8	WHITE	0	857	0	2054	0	857	0	2054	1	297	3	299
16	9	WHITE	4	18430	0	37074	6107	18430	0	30971	155	166	134	145
16	10	WHITE	0	1214	0	1911	577	1214	0	1334	185	138	162	115
16	11	WHITE	754799	0	0	0	754799	0	0	0	300	0	0	0
17	8	WHITE	0	3050	0	0	0	3050	0	0	0	299	1	0
17	9	WHITE	0	8030	0	0	0	8030	0	0	0	153	147	0
17	12	WHITE	0	3	0	0	0	3	0	0	0	0	2	0
18	9	WHITE	0	109535	0	0	0	109535	0	0	0	153	147	0
18	13	WHITE	0	4005	0	0	0	4005	0	0	0	228	72	0
19	9	WHITE	0	31803	0	0	0	31803	0	0	0	187	113	0
19	13	WHITE	0	4492	0	0	0	4492	0	0	0	223	77	0
20	9	WHITE	0	19142	0	0	0	19142	0	0	0	174	126	0
20	13	WHITE	0	46653	0	0	0	46653	0	0	0	173	127	0
21	9	WHITE	0	24465	0	0	0	24465	0	0	0	300	0	0
22	9	WHITE	0	86891	0	0	0	86891	0	0	0	300	0	0
23	9	WHITE	0	7504	0	4278	275	7504	0	4003	105	43	257	195
23	24	WHITE	0	1765	0	40	15	1765	0	25	36	207	93	3
24	9	WHITE	0	7754	0	470	123	7754	0	347	229	24	276	71
24	27	WHITE	0	1856	0	20	8	1856	0	12	18	226	74	1
25	9	WHITE	0	41653	0	0	0	41653	0	0	0	196	104	0
25	25	WHITE	0	111	0	0	0	111	0	0	0	52	58	0
25	26	WHITE	0	100	0	0	0	100	0	0	0	90	9	0
25	28	WHITE	0	1484	0	0	0	1484	0	0	0	96	204	0
25	29	WHITE	0	1	0	0	0	1	0	0	0	0	0	0
25	30	WHITE	0	1916	0	0	0	1916	0	0	0	80	220	0
25	31	WHITE	0	1468	0	0	0	1468	0	0	0	121	179	0
25	32	WHITE	0	1962	0	0	0	1962	0	0	0	105	195	0
25	33	WHITE	0	1557	0	0	0	1557	0	0	0	144	156	0
25	34	WHITE	0	0	0	0	0	0	0	0	0	0	0	0
25	35	WHITE	0	0	0	0	0	0	0	0	0	0	0	0
25	36	WHITE	0	0	0	0	0	0	0	0	0	0	0	0

1. **Подход:** формирование белых списков системных вызовов.

2. Подход: формирование белых списков системных вызовов и их аргументов.

3. Подход: формирование белых списков последовательности системных вызовов.

Тестирование подходов обнаружения

16	8	BLACK	0	857	0	2054	0	857	0	2054	0	300	0	300
16	9	BLACK	4	18430	0	37074	6107	18430	0	30971	19	286	14	281
16	10	BLACK	0	1214	0	1911	577	1214	0	1334	83	253	47	217
16	11	BLACK	754799	0	0	0	754799	0	0	0	285	0	0	15
17	8	BLACK	0	3050	0	0	0	3050	0	0	0	300	0	0
17	9	BLACK	0	8030	0	0	0	8030	0	0	0	300	0	0
17	12	BLACK	0	3	0	0	0	3	0	0	0	2	0	0
18	9	BLACK	0	109535	0	0	0	109535	0	0	0	300	0	0
18	13	BLACK	0	4005	0	0	0	4005	0	0	0	300	0	0
19	9	BLACK	0	31803	0	0	0	31803	0	0	0	300	0	0
19	13	BLACK	0	4492	0	0	0	4492	0	0	0	300	0	0
20	9	BLACK	0	19142	0	0	0	19142	0	0	0	300	0	0
20	13	BLACK	0	46653	0	0	0	46653	0	0	0	300	0	0
21	9	BLACK	0	24465	0	0	0	24465	0	0	0	300	0	0
22	9	BLACK	0	86891	0	0	0	86891	0	0	0	300	0	0
23	9	BLACK	0	7504	0	4278	275	7504	0	4003	11	181	119	289
23	24	BLACK	0	1765	0	40	15	1765	0	25	4	294	6	35
24	9	BLACK	0	7754	0	470	123	7754	0	347	95	255	45	205
24	27	BLACK	0	1856	0	20	8	1856	0	12	9	299	1	10
25	9	BLACK	0	41653	0	0	0	41653	0	0	0	300	0	0
25	25	BLACK	0	111	0	0	0	111	0	0	0	110	0	0
25	26	BLACK	0	100	0	0	0	100	0	0	0	99	0	0
25	28	BLACK	0	1484	0	0	0	1484	0	0	0	300	0	0
25	29	BLACK	0	1	0	0	0	1	0	0	0	0	0	0
25	30	BLACK	0	1916	0	0	0	1916	0	0	0	300	0	0
25	31	BLACK	0	1468	0	0	0	1468	0	0	0	300	0	0
25	32	BLACK	0	1962	0	0	0	1962	0	0	0	300	0	0
25	33	BLACK	0	1557	0	0	0	1557	0	0	0	300	0	0
25	34	BLACK	0	0	0	0	0	0	0	0	0	0	0	0
25	35	BLACK	0	0	0	0	0	0	0	0	0	0	0	0
25	36	BLACK	0	0	0	0	0	0	0	0	0	0	0	0

1. **Подход:** формирование черных списков системных вызовов.

2. Подход: формирование черных списков системных вызовов и их аргументов.

3. Подход: формирование черных списков последовательности системных вызовов.

Тестирование подходов обнаружения

1. Подход:
Почти не работает.
Подход обнаружил аномалии в контейнерах, где нет ничего, кроме аномалии (что довольно просто). Но не сказать, что он на 100% непригоден для использования.
Самый быстрый подход.
Списки весят < 1 КБ.

3. Подход:
Работает, но в белом списке есть ложные срабатывания.
Обнаружил все аномалии и атаки.
Подход работает в течение нескольких минут.
Списки весят < 1 МБ

2. Подход:
Работает лучше всего.
Ложных срабатываний не бывает. По сравнению с другими, здесь меньше ложных срабатываний.
Подход работает в течение нескольких минут.
Списки весят > 1 МБ

Результаты исследования

1. Проведено тестирование систем сбора данных с поддержкой зонда eBPF.
2. Сформированы наборы данных с аномальной и нормальной активностью.
3. Сформированы наборы данных с нормальной активностью и атаками.
4. Разработаны новые подходы обнаружения аномалий и атак:
   a. Формирование черных и белых списков событий;
   b. Формирование черных и белых списков событий и их аргументов;
   c. Формирование черных и белых списков последовательности событий.
5. Проведено тестирование подходов обнаружения аномалий и атак

Перспективные задачи и исследования

1. Могут быть созданы программы сбора для каждого подхода или сигнатуры атаки (поддержкой зонда eBPF).
2. Необходимо сформировать большее количество наборов данных для тестирования.
3. Возможно разработать такой подход, который позволит формировать сигнатуры для атак на основе обнаруженных аномалий.
4. Необходимо провести нагрузочное и функциональное тестирование комплексного подхода для сравнения с известными методами обнаружения.

Спасибо за внимание!