

Ampire 360°



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





# Битва ИИнтеллектов. Как изменится наше цифровое будущее

Александр Пушкин

Заместитель генерального директора  
Перспективный мониторинг

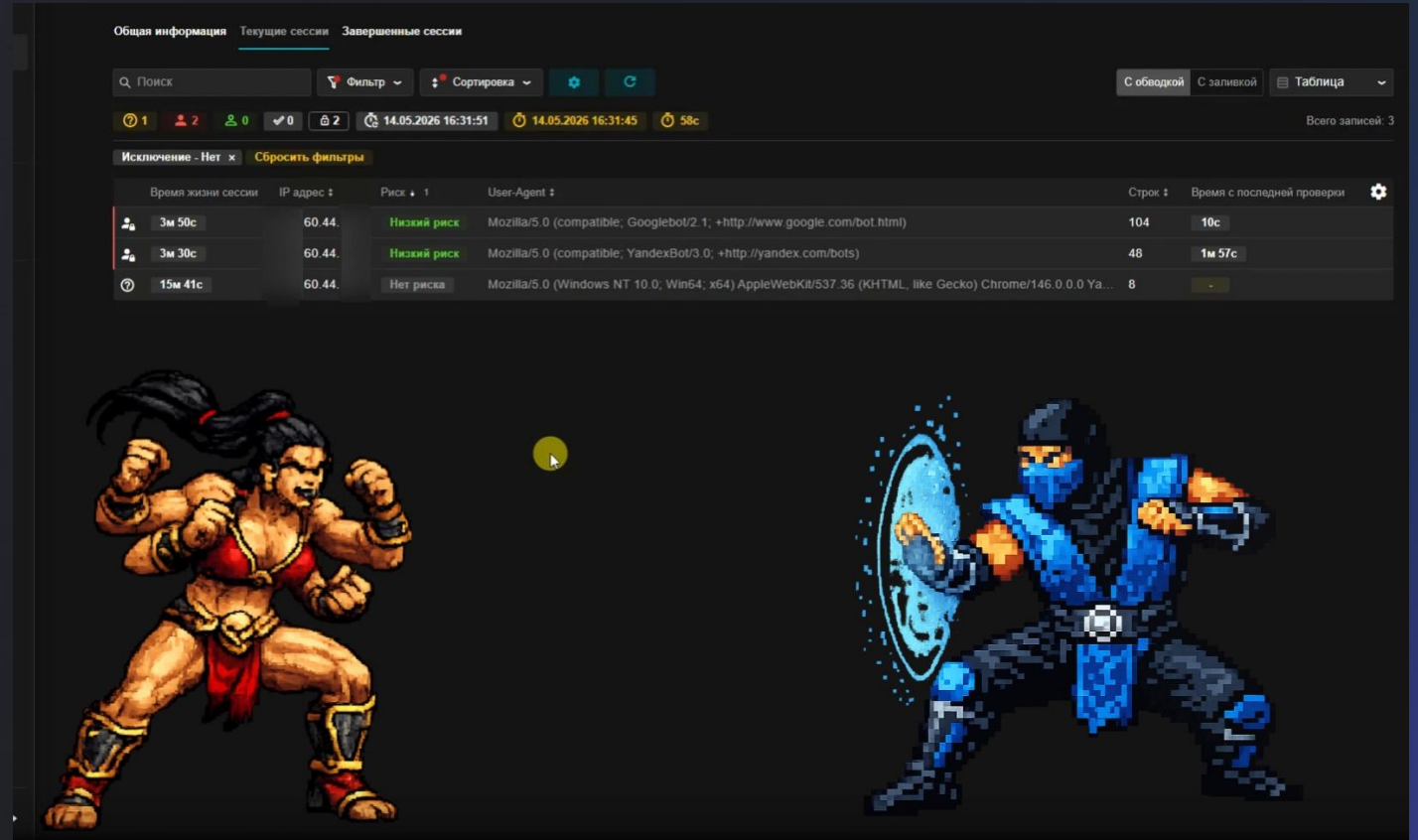


# Эксперимент будущего



# Идея

1. Со стороны атаки: ИИ-комбайн
2. Со стороны защиты: AML Web Protection
3. Объект атаки: уязвимый узел из Ampire



# Техническая реализация

Ampire 360°



## ИИ-комбайн:

- Несколько LLM
- ИИ-агенты
- >150 инструментов через MCP



- Drupalgeddon
- NPM
- Apache Proxy



## AML Web Protection

- Анализ журнала веб-сервера
- ML-модель
- Блокировка

# Цели эксперимента

1. Принципиальная возможность схемы  
машина — машина
2. Увидеть в деталях работу ИИ при атаке
3. Понять точки роста для AML



# Аккуратная разведка

Общая информация

Атакующая сессия

Низкий риск

Начало: 09.10.2026 14:55:33

Завершение: 09.10.2026 14:55:54

Длительность: 00:00:21

Предсказание подтверждено

Да

Нет

Парсер: Combined

Версия модели: 23-09-2026\_10

Строк: 10

Файл с логами: [Скачать](#)

Риск подтвержден

Да

Нет

Логи сессии (10)

Подсвеченные

Декодировать - Да x

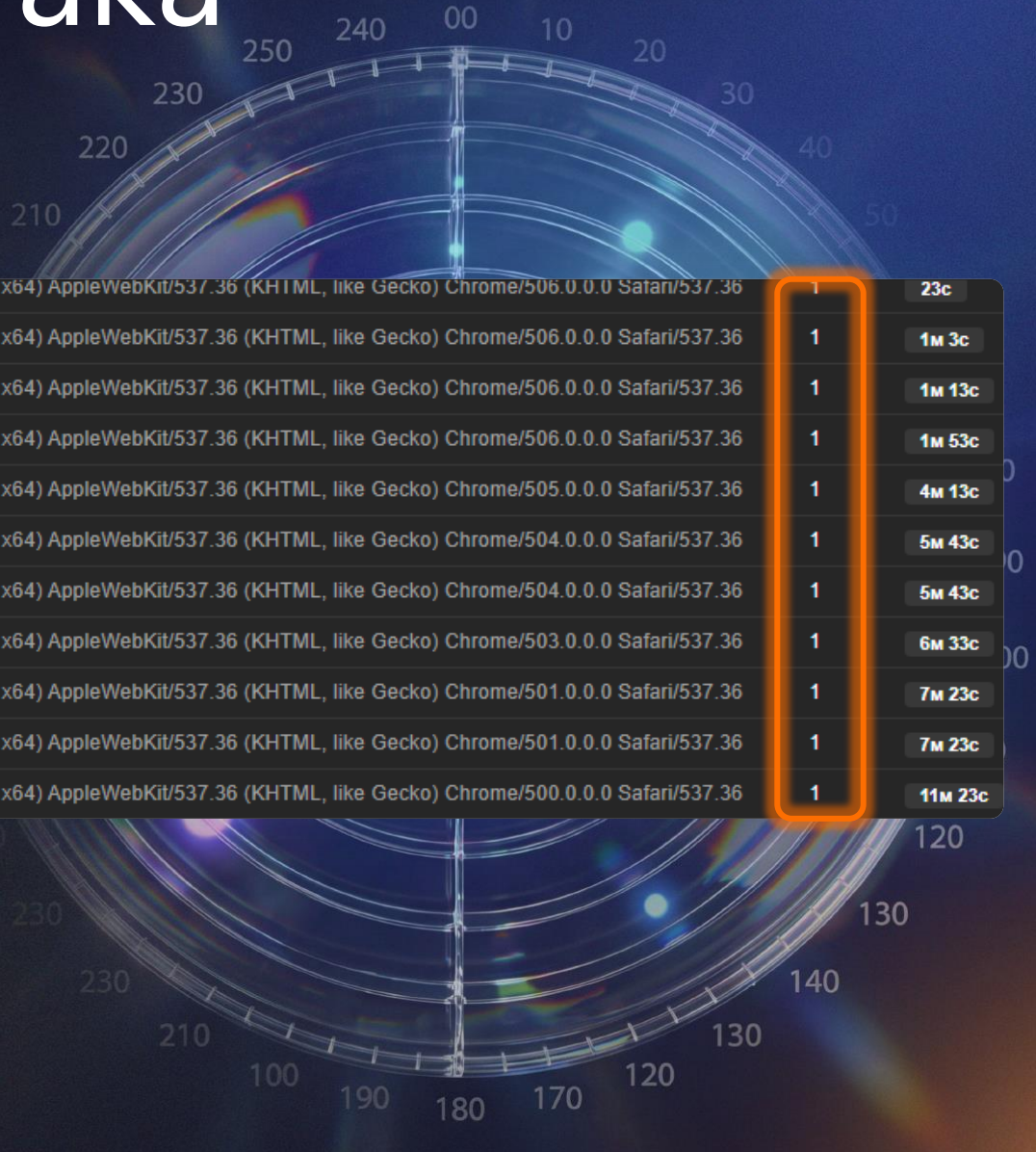
Только именованные атрибуты - Да x

Сбросить фильтры

|    |       |   |                              |                            |     |     |   |                                                                                                                 |
|----|-------|---|------------------------------|----------------------------|-----|-----|---|-----------------------------------------------------------------------------------------------------------------|
| 1  | 1.146 | - | [09/Oct/2026:11:55:33 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 2  | 1.146 | - | [09/Oct/2026:11:55:35 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 3  | 1.146 | - | [09/Oct/2026:11:55:37 +0000] | GET //phpinfo.php HTTP/1.1 | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 4  | 1.146 | - | [09/Oct/2026:11:55:39 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 5  | 1.146 | - | [09/Oct/2026:11:55:41 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 6  | 1.146 | - | [09/Oct/2026:11:55:43 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 7  | 1.146 | - | [09/Oct/2026:11:55:45 +0000] | GET /phpinfo.php/ HTTP/1.1 | 404 | 326 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 8  | 1.146 | - | [09/Oct/2026:11:55:48 +0000] | GET /PhplInfo.php HTTP/1.1 | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 9  | 1.146 | - | [09/Oct/2026:11:55:52 +0000] | GET /.phpinfo.php HTTP/1.1 | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |
| 10 | 1.146 | - | [09/Oct/2026:11:55:54 +0000] | GET /phpinfo.php HTTP/1.1  | 403 | 552 | - | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 |

# Распределенная атака

Ampire 360°



|   |                     |         |                 |           |                                                                                                                 |   |         |
|---|---------------------|---------|-----------------|-----------|-----------------------------------------------------------------------------------------------------------------|---|---------|
| 👤 | 09.10.2026 17:23... | 34с     | 192.42.116.101  | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/506.0.0.0 Safari/537.36 | 1 | 23с     |
| 👤 | 09.10.2026 17:23... | 1м 18с  | 80.67.172.162   | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/506.0.0.0 Safari/537.36 | 1 | 1м 3с   |
| 👤 | 09.10.2026 17:23... | 1м 20с  | 192.42.116.60   | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/506.0.0.0 Safari/537.36 | 1 | 1м 13с  |
| 👤 | 09.10.2026 17:22... | 2м 2с   | 192.42.116.58   | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/506.0.0.0 Safari/537.36 | 1 | 1м 53с  |
| 👤 | 09.10.2026 17:20... | 4м 23с  | 193.189.100.200 | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/505.0.0.0 Safari/537.36 | 1 | 4м 13с  |
| 👤 | 09.10.2026 17:18... | 5м 49с  | 185.220.101.23  | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/504.0.0.0 Safari/537.36 | 1 | 5м 43с  |
| 👤 | 09.10.2026 17:18... | 5м 51с  | 185.220.101.110 | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/504.0.0.0 Safari/537.36 | 1 | 5м 43с  |
| 👤 | 09.10.2026 17:17... | 6м 42с  | 192.42.116.113  | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/503.0.0.0 Safari/537.36 | 1 | 6м 33с  |
| 👤 | 09.10.2026 17:16... | 7м 33с  | 192.42.116.48   | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/501.0.0.0 Safari/537.36 | 1 | 7м 23с  |
| 👤 | 09.10.2026 17:16... | 7м 34с  | 5.2.67.226      | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/501.0.0.0 Safari/537.36 | 1 | 7м 23с  |
| 👤 | 09.10.2026 17:12... | 11м 40с | 192.42.116.106  | Нет риска | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/500.0.0.0 Safari/537.36 | 1 | 11м 23с |

# Результативный эксплойт

|    |        |   |   |                              |                                       |     |      |                      |
|----|--------|---|---|------------------------------|---------------------------------------|-----|------|----------------------|
| 34 | 44.146 | - | - | [09/Oct/2026:14:53:55 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 35 | 44.146 | - | - | [09/Oct/2026:14:54:08 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 36 | 44.146 | - | - | [09/Oct/2026:14:54:19 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 37 | 44.146 | - | - | [09/Oct/2026:14:54:29 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 38 | 44.146 | - | - | [09/Oct/2026:14:54:41 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 39 | 44.146 | - | - | [09/Oct/2026:14:54:52 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 40 | 44.146 | - | - | [09/Oct/2026:14:55:03 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 41 | 44.146 | - | - | [09/Oct/2026:14:55:14 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 42 | 44.146 | - | - | [09/Oct/2026:14:55:26 +0000] | GET /pwned.txt HTTP/1.1               | 200 | 1693 | - Python-urllib/3.12 |
| 43 | 44.146 | - | - | [09/Oct/2026:14:58:05 +0000] | POST /api/nginx/certificates HTTP/1.1 | 500 | 961  | - Python-urllib/3.12 |
| 44 | 44.146 | - | - | [09/Oct/2026:14:58:57 +0000] | POST /api/nginx/certificates HTTP/1.1 | 500 | 961  | - Python-urllib/3.12 |
| 45 | 44.146 | - | - | [09/Oct/2026:14:58:57 +0000] | GET /hn.txt HTTP/1.1                  | 200 | 13   | - Python-urllib/3.12 |
| 46 | 44.146 | - | - | [09/Oct/2026:14:58:57 +0000] | GET /pw.txt HTTP/1.1                  | 200 | 878  | - Python-urllib/3.12 |

# Прогноз



# 1. Атакующие будут быстрее внедрять ИИ

1. Разведка->Первоначальный доступ->Закрепление->Развитие->Работа внутри
2. Минимальные потери на первых этапах
3. «Небольшие» вычислительные ресурсы\*
4. Автоматическая подготовка инструментов
5. Монетизация сервиса ИИ для атаки

## 2. Сначала ML, а ИИ контролирует для защиты

1. Надо «лопатить» гигабайты данных, и очень быстро
2. Цена ошибки велика
3. Требуется прозрачность работы машины

# 3. Цена ошибки увеличивается для владельца ИС

1. Отсутствие человеческого фактора у ИИ, чтобы «докрутить» уязвимость
2. Скорость подготовки **кастомного эксплойта** на порядок выше
3. Широкий набор компетенций

Спасибо  
за внимание



Ampire 360°