

Ampire 360°



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





# SOC + TI:

как эффективно выстроить  
взаимодействие

Александр Рудзик

Руководитель направления исследований  
киберугроз

Перспективный мониторинг



# Профили работы команд

## Security Operations Center (SOC)

- Непрерывный мониторинг
- Triage и приоритизация
- Обнаружение инцидентов
- Эскалация (L1 → L2 → L3) и реагирование
- Документирование процессов и отчётность

## Threat Intelligence (TI)

- Сбор данных (collection)
- Анализ и обогащение IoCs
- Оценка TTP злоумышленников
- Поддержка решений
- Совершенствование инструментов



# Преимущества команд

## Security Operations Center (SOC)

- Ключевое преимущество — прямой доступ к реальной инфраструктуре
- Вторая ценность — возможность мгновенно действовать на основе этого доступа
- Третье преимущество — точные и проверенные данные

## Threat Intelligence (TI)

- Ключевое преимущество — проактивность вместо реактивности. Команда позволяет видеть картину угроз извне до того, как они дойдут до инфраструктуры
- Вторая ценность — накопленные знания дают быстрый и точный контекст. За годы работы команда формирует глубокое понимание методов злоумышленников, их мотивации и инфраструктуры



# Взаимодействие команд



## Запросы для разработки правил

На основе известной инфраструктуры формируется приоритизация угроз и уязвимостей

## Вредоносная активность

Передача событий и логов для обогащения информацией

## Фишинговые письма и ВПО

Передача реальных артефактов на дополнительный анализ

## False Positive-сработки

Оповещение о наличии или отсутствии событий безопасности

# SOC → TI

Добрый день! Просьба создать правила на следующие уязвимости:

CVE-2026-47291

Описание: Уязвимость в Windows HTTP.sys позволяет удаленно выполнить произвольный код

Критичность: 9.8 Critical

Источник: <https://nvd.nist.gov/vuln/detail/CVE-2026-47291>

CVE-2026-48939

Описание: Joomla расширение "iCagenda" содержит уязвимость, позволяющую злоумышленнику загрузить и исполнить произвольный файл.

Критичность: 9.8 Critical

Источник: <https://nvd.nist.gov/vuln/detail/CVE-2026-48939>

CVE-2026-56291

Описание: Joomla расширение "Balboa Forms" содержит уязвимость, позволяющую злоумышленнику загрузить и исполнить произвольный файл.

Критичность: 9.8 Critical

Источник: <https://nvd.nist.gov/vuln/detail/CVE-2026-56291>

13:07



Вирус\_23\_04\_2026.7z

7.02 МБ

Коллеги, добрый день!

Получили интересное письмо. Возможно будет полезно для анализа

Пароль: [REDACTED]

09:36



Инструктаж.7z

6.77 МБ

Пароль: [REDACTED]

11:23

SOC

Коллеги, добрый день!

Фиксируем нестандартную активность powershell. Сможем атрибутировать?

18:34



logs.xml

4 Б

18:34

Коллеги, добрый день! Наблюдаем большое количество ложноположительных срабатываний следующих правил:

- 1) SID:3434767
- 2) SID:2069174
- 3) SID:2069175

11:25



953993575-192.168.252.211-3434767.p...

296 Б

SID:3434767

11:26



951361899-192.168.252.211-2069174.p...

142 Б

SID:2069174

11:26



951361900-192.168.252.211-2069175.p...

142 Б

SID:2069175

11:26

SOC

# TI → SOC

## Тактический уровень

Индикаторы компрометации,  
индикаторы атак

## Операционный уровень

Используемые инструменты,  
шаблоны поведения

## Стратегический уровень

Вредоносная активность группировок,  
их мотивы и цели

## Инфраструктурные запросы

Запросы с целью уточнения наличия  
ПО и защищаемых отраслей

# TI → SOC

## Тактический уровень

Индикаторы компрометации,  
индикаторы атак

### AM TI Feeds

```
1 {
2   "id": "bundle--725fa9e4-fcdc-4884-815c-4b889d0bd5db",
3   "spec_version": "2.1",
4   "type": "bundle",
5   "objects": [
6     {
7       "id": "domain-name--20721b12-3a87-4c1d-bfce-21d0e0d7554d",
8       "spec_version": "2.1",
9       "type": "domain-name",
10      "name": "accountservices.nl",
11      "value": "accountservices.nl",
12      "top_level_domain": "nl",
13      "history": {
14        "uploaded": "2025-06-15T01:01:30Z",
15        "updated": "2026-09-21T11:09:34Z"
16      }
17    },
18    {
19      "id": "indicator--00ffda38-b1b2-4df4-8dec-1ddc4cadd95d",
20      "spec_version": "2.1",
```

### AM Rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Observed Librarian Ghoul Domain (accountservices .nl in
TLS SNI)"; flow:established,to_server; content:"|16|"; content:"|01|"; within:8; content:"|00 00|"; distance:0;
content:"|00|"; distance:4; within:1; byte_jump:2,0,relative, post_offset -19;
pcrc:"/^(?:\x00\x11|\x2e)accountservices\.nl/R"; content:"accountservices.nl"; fast_pattern:only;
reference:url,securelist.com/librarian-ghouls-apt-wakes-up-computers-to-steal-data-and-mine-crypto/116536/;
classtype:trojan-activity; sid:2065327; rev:1; metadata: affected_asset src, affected_product n/a, affected_vendor
n/a, attack_target Client_Endpoint, confidence High, created_at 2025_10_22, deployment Perimeter, signature_severity
medium, tias_category Malware, updated_at 2025_10_22;)
```

```
name:'value' = 'accountservices.nl' ]",
-21T11:09:34Z",
1-02T11:09:34Z"
71faaa6-f457-4a90-8006-862828ce5579",
indicates",
cor--00ffda38-b1b2-4df4-8dec-1ddc4cadd95d",
name--20721b12-3a87-4c1d-bfce-21d0e0d7554d"
```

# TI → SOC

## Операционный уровень

Используемые инструменты,  
шаблоны поведения

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"AM USER_AGENTS
[HUNT] Suspicious User Agent Hoody Hyena (BrokenDoor)";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla/5.0 (X11\; U\;
Linux i686\; pl\; rv:1.8.1) Gecko/20061010 Firefox/2.0"; http_header;
reference:cve,NA; reference:url,bi.zone/expertise/blog/kak-ispolzovat-
kiberrazveddannye-dlya-obnaruzheniya-ugroz; classtype:trojan-activity;
sid:3436463; rev:1; metadata: affected_asset src, affected_os any,
affected_product n/a, affected_vendor n/a, attack_target Client_Endpoint,
created_at 2026_07_21, malware_name BrokenDoor, signature_severity medium, tag
T1071, tag TA0011, tias_category Malware, updated_at 2026_07_21;)
```

```
<rule id="400502" level="2">
  <id>^4104$</id>
  <regex ignorecase="true">ScriptBlockText.+(Schedule\.Service)?\.(NewTask|New-ScheduledTask)\.(RegisterTaskDefinition|Register-ScheduledTask)</regex>
  <description>Обнаружено создание и запуск задачи планировщика через powershell</description>
  <info>
    <link>app.any.run/tasks/a9dc6d6f-8d11-4420-bed2-995763523d24</link>
    <techniques>T1053.005,T1059.001</techniques>
    <capec></capec>
    <cwe></cwe>
    <cve></cve>
  </info>
  <category>suspicious_activity</category>
</rule>
```

# TI → SOC

## Стратегический уровень

### Вредоносная активность группировок, их мотивы и цели

Коллеги, добрый день! Информировуем об активности группировки room155/DarkGaboorn

Из последних материалов:

- [https://amonitoring.ru/article/stat\\_spetsialistom\\_po\\_issledovaniyu\\_kiberugroz\\_na\\_odin\\_post](https://amonitoring.ru/article/stat_spetsialistom_po_issledovaniyu_kiberugroz_na_odin_post)
- [https://1275.ru/ioc/vengeful-wolf-ataket-gosorgany-rf-cherez-fishing-s-revenge-rat\\_16787](https://1275.ru/ioc/vengeful-wolf-ataket-gosorgany-rf-cherez-fishing-s-revenge-rat_16787)
- <https://www.f6.ru/blog/room155/>

Краткая сводка:

- Вектор первоначального доступа: рассылка фишинговых писем с вредоносным вложением в виде zip-архива. Архив содержит отвлекающий документ с расширением ".doc", а также исполняемый файл с расширением ".exe". Темы писем, а также названия исполняемых файлов имеют отличительную черту в наименовании: "Акт сверки взаиморасчетов"/ "Акт сверки взаимных расчетов предприятия № 420 от 23 июня 2026 года.exe".

- Инструментарий: Revenge RAT, LockBit, XWorm, VenomRAT - набор из последних кампаний группировки. Также замечено применение: Warzor
- Отрасли: Информационные технологии, Транспорт, Связь, Финансы, Розничная торговля, Электронная коммерция, Государственное управление

Индикаторы компрометации (IOC's), зафиксированные за последний месяц, прикреплены в отдельных файлах

Сетевые IOC's также добавлены в БРП, хэши в базу Malware Detection

Коллеги, добрый день! Информировуем об активности группировки room155/DarkGaboorn...

hashes\_room155.txt  
1.29 КБ

11:17

Коллеги, добрый день! Информировуем об активности группировки room155/DarkGaboorn...

network\_iocs\_room155.txt  
150 Б

11:17

Информирую) Есть информация, что активизировались PhantomCore

Из последних докладов (ГосСОПКА):

- [https://cdn.ib-bank.ru/sopka/materials/15/Opyt\\_reagirovaniya\\_na\\_kompyuternye\\_intsidenty/Dyomochkin\\_Lantaev\\_Gurevich.pdf](https://cdn.ib-bank.ru/sopka/materials/15/Opyt_reagirovaniya_na_kompyuternye_intsidenty/Dyomochkin_Lantaev_Gurevich.pdf)
- [https://cdn.ib-bank.ru/sopka/materials/14/Tekhnologicheskii\\_trek/Grigoryan\\_Khandozhko.pdf](https://cdn.ib-bank.ru/sopka/materials/14/Tekhnologicheskii_trek/Grigoryan_Khandozhko.pdf)

Краткая сводка:

- Инструментарий: ADRecon, Babuk, CVE-2017-0147, CVE-2023-23397, CVE-2023-38831, LockBit, Mimikatz, Ngrok, NSSM, Ntdsutil, PhantomDL, PhantomRAT, Persey, P0wny Shell, rsockstun, Sliver, Sherlock, XenArmor All-In-One Password Recovery Pro, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, secretsdump, ProcDump, Localtonet, revsocks, cloudflared, Gost, fscan, SoftPerfect Network Scanner, mRemoteNG, PSEXec, smbexec, wmiexec, CobInt, PhantomJitter, rclone, PhantomPyramid, MeshAgent (MeshCentral), StatRAT, PhantomRemote, PhantomStealer, T1ck3tDump, PhantomTaskShell, rsocx, OpenSSH, Impacket, Certify, PAExec, PhantomProxyLite, ADEplorer, Advanced IP Scanner, DumpIt, memprocs, BDU:2025-10114, BDU:2025-10116, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, MicroSocks, HeartDoor, HeartDoorLite, KermitRAT

- Отрасли: Информационные технологии, Инженерия, Отрасль добычи полезных ископаемых, Наука, Транспорт, Государственное управление, Энергетика, Связь, СМИ, Электронная коммерция, Обрабатывающая промышленность, Финансы, Здравоохранение, Розничная торговля, Организация досуга и развлечений

Archive update! Added leaked data of 1 russian building materials company: [литокс.рф](https://litoкс.рф) and 3 russian airports: [airportbaikal.ru](https://airportbaikal.ru), [ulk.aero](https://ulk.aero), [rgk-aero.ru](https://rgk-aero.ru)! [dropbox.com/scl/fi/r7uvgrh...](https://dropbox.com/scl/fi/r7uvgrh...)



# TI → SOC

Ampire 360°

## Инфраструктурные запросы

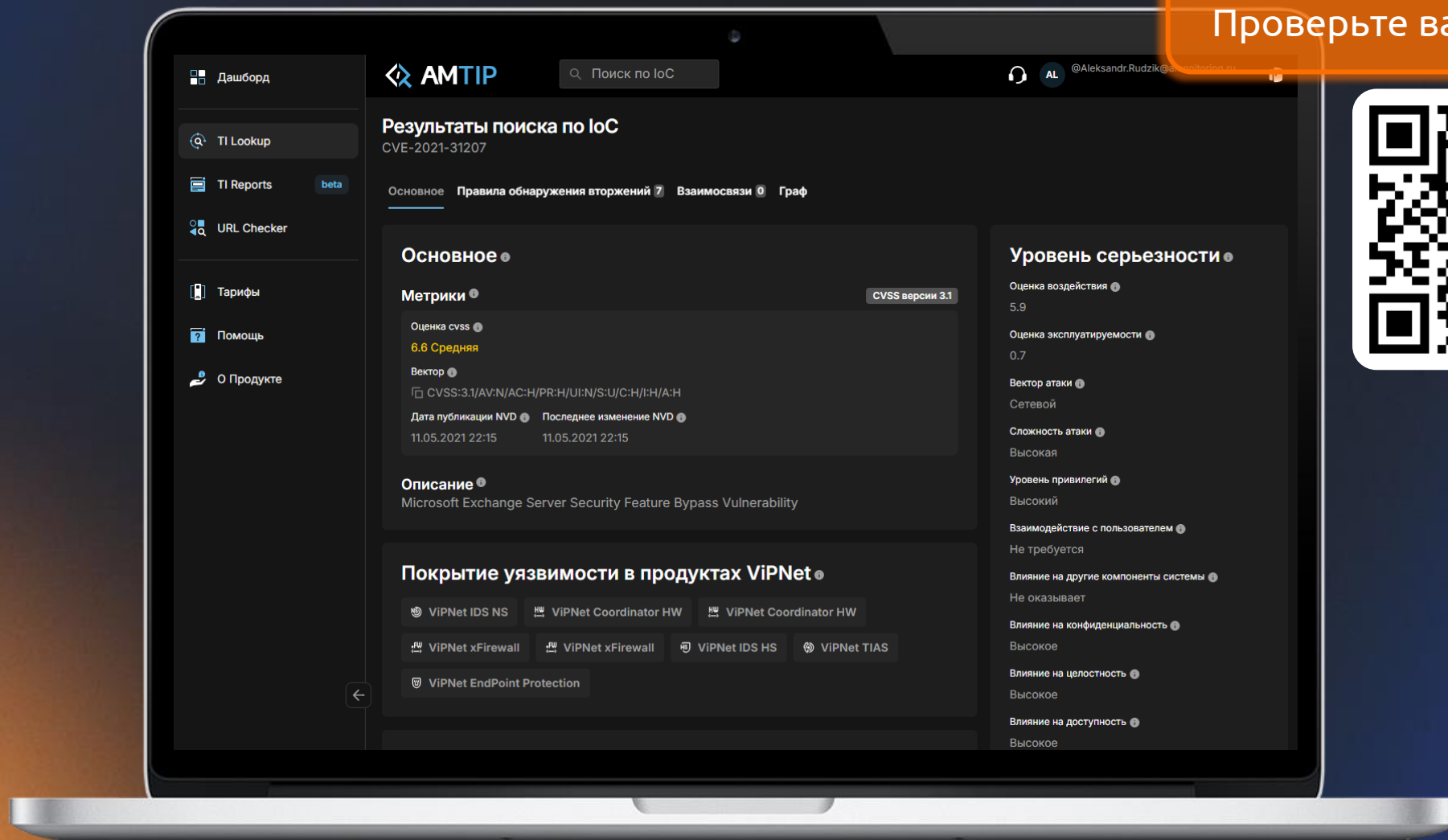
Запросы с целью уточнения  
наличия ПО и защищаемых  
отраслей



# Распространение информации

Ampire 360°

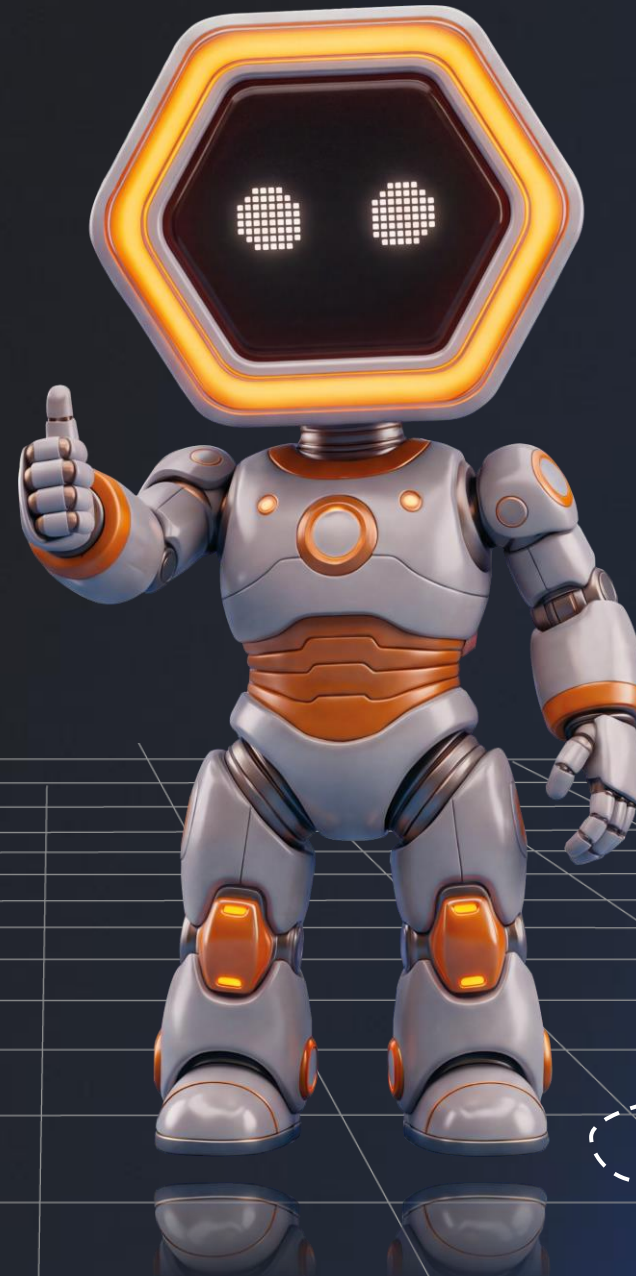
Проверьте ваши IoCs



# Благодарю за внимание!

Александр Рудзик

Руководитель направления  
исследований киберугроз



Остались вопросы?

Ampire 360°