

APT-атаки на промышленные компании в первом полугодии 2021 года

SolarWinds	2
Cicada/APT10.....	3
Andariel.....	4
Группы, связанные с Китаем.....	5
Атаки ReverseRat в Индии и Афганистане.....	6
Operation Spalax	7
Новые примеры активности Lazarus.....	8
RedEcho/ShadowPad.....	9
Zebrocy	9
Атака на иранские центрифуги.....	10
Атаки на аэрокосмическую отрасль с использованием утилит удаленного доступа (RAT)	10
Gelsemium	11
Заключение	12

В этом обзоре описаны основные АРТ-атаки на промышленные организации, сведения о которых были опубликованы в первой половине 2021 года, и соответствующая деятельность группировок, замеченных в атаках на промышленные организации и критическую инфраструктуру. Для каждой истории мы постарались суммировать наиболее значимые факты, находки и выводы исследователей, которые, на наш взгляд, могут быть полезны экспертам, решающим практические задачи обеспечения кибербезопасности промышленных предприятий.

SolarWinds

В нашем предыдущем [отчете об APT-атаках](#) была описана крупномасштабная и сложная атака на цепочку поставок с эксплуатацией уязвимостей в ПО для промышленных предприятий Orion IT компании SolarWinds. Исследователи продолжили анализ этой кампании и получили новые результаты.

Были обнаружены новые семейства вредоносного ПО. Первое, получившее название [Sunspot](#), было задействовано в сентябре 2019 года, когда злоумышленники впервые проникли в сеть компании. Это вредоносное ПО было установлено на сервере сборки SolarWinds и было предназначено для перехвата на сервере команд на сборку продукта Orion. При обнаружении команды на сборку продукта Orion вредоносное ПО Sunspot скрытно подменяло файл с исходным кодом, содержащим загрузчик вредоносного ПО Sunburst. Второе семейство, названное [Raindrop](#), — это загрузчик бэкдора, устанавливающий Cobalt Strike на уже зараженной системе, чтобы обеспечить распространение вредоносного ПО через целевую сеть. Компания Microsoft также опубликовала [новый анализ](#) вредоносного ПО, примененного в данной атаке, описывающий, в частности, ее недостающее звено — последовательность процессов, позволяющих передать управление от бэкдора Sunburst загрузчику Cobalt Strike. Атакующие разделили эти два компонента настолько сильно, насколько это было возможно, чтобы избежать обнаружения. Кроме того, в исследовании Microsoft уже опубликованные сведения о тактиках, приемах и процедурах, использованных злоумышленниками, дополнены описанием дополнительных хакерских (hands-on-keyboard) приемов, примененных атакующими в ходе первоначальной разведки, сбора данных и их вывода с атакованных систем.

Позднее были обнаружены новые семейства вредоносного ПО, применяемые группировкой, стоящей за атакой SolarWinds. Среди них — бэкдор GoldMax (известный также как [Sunshuttle](#)), а также [Sibot](#) и [GoldFinder](#).

Швейцарская компания Prodaft, специализирующаяся на проблемах кибербезопасности, опубликовала [исследование](#), в котором описывается активность обнаруженной ей группировки, получившей название SilverFish. В отчете утверждается, что эта группировка имеет отношение к инцидентам SolarWinds (исследователи считают, что за инцидентами стоят несколько группировок, каждая с собственными мотивами для атаки). Данная группировка ответственна за атаки более чем на 4720 частных и государственных организаций, в число которых входят компании из списка Fortune 500, министерства, авиакомпании, военные подрядчики, аудиторские и консалтинговые фирмы, а также автопроизводители.

Группировка SilverFish вела широкомасштабную кампанию с августа 2020 года по март 2021 года. Исследователям Prodaft удалось получить доступ к одному из командных серверов группировки. Эксперты нашли на сервере ценную информацию о жертвах атаки и активности злоумышленников после заражения систем. Наиболее необычная обнаруженная активность — использование существующих предприятий-жертв в качестве «песочницы» для тестирования вредоносных модулей на обнаружение корпоративными EDR и антивирусными решениями с отправкой результатов проверки обратно на сервер.

Cicada/APT10

В ноябре–декабре 2020 года компании [Symantec](#) и [LAC](#) опубликовали блогпосты о кампании группировки APT10. Месяц спустя эксперты «Лаборатории Касперского» [обнаружили](#) новую активность этой группировки с применением обновленной версии некоторых имплантов, позволяющей более эффективно избегать обнаружения защитными продуктами и усложняющей исследователям анализ вредоносного ПО.

«Лаборатория Касперского» провела расследование длительной кампании кибершпионажа, получившей название A41APT и затронувшей несколько отраслей, в том числе японских производителей и их зарубежные объекты. Кампания активна с марта 2019 года. Злоумышленники использовали уязвимости в [продукте SSL VPN](#) для установки многоступенчатого загрузчика, получившего название Ecipekas (другие его названия: DESLoader, SigLoader и HEAVYHAND). Большинство обнаруженных вредоносных нагрузок, доставляемых этим загрузчиком, — это бесфайловые вредоносные программы, которые ранее не встречались. Были обнаружены следующие вредоносные программы: SodaMaster (она же DelfsCake, dfls и DARKTOWN), P8RAT (она же GreetCake и HEAVYPOT) и FYAnti (она же DILLJUICE Stage 2). Последняя в свою очередь загружает QuasarRAT — популярную утилиту удаленного администрирования с открытым исходным кодом.

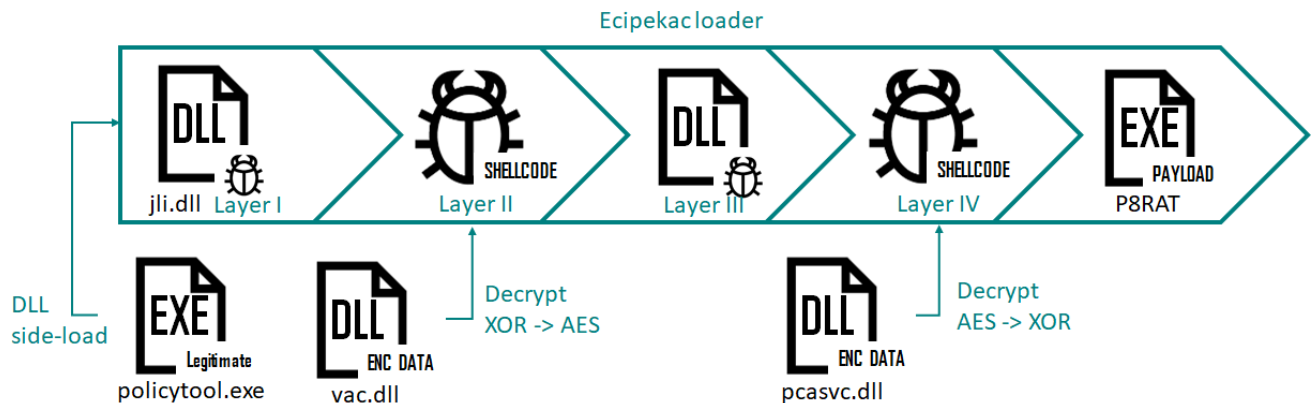


Схема заражения Еcipeкас (Источник: [«Лаборатория Касперского»](#))

Andariel

Эксперты «Лаборатории Касперского» [обнаружили](#) активность группировки Andariel, нацеленную на широкий круг отраслей экономики Южной Кореи, включая промышленность, услуги домашнего интернета, СМИ и строительство, с использованием обновленной схемы заражения и, в одном случае, нестандартной программы-вымогателя. В апреле эксперты компании обнаружили документ-приманку с корейским именем файла, загруженный на сервис VirusTotal. В результате были выявлены новая схема заражения и не встречавшаяся ранее вредоносная нагрузка.

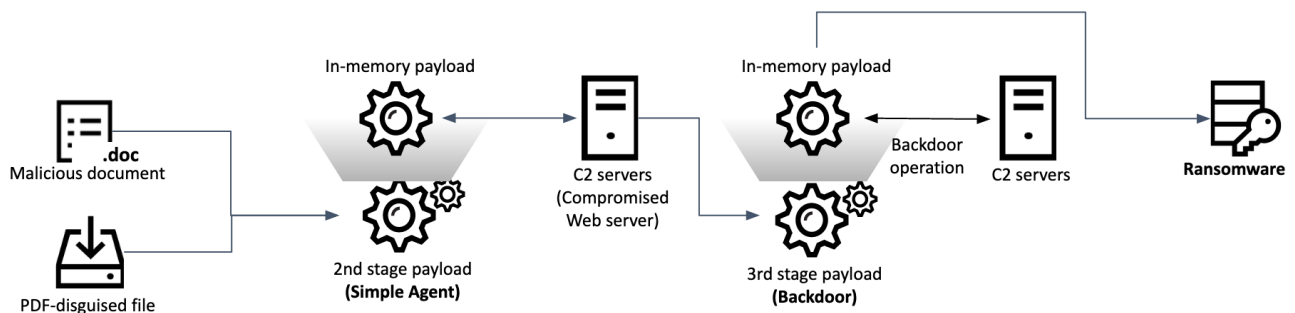


Схема заражения (Источник: [«Лаборатория Касперского»](#))

Группировка распространяет вредоносную нагрузку третьего этапа с середины 2020 года и использовала в качестве векторов заражения вредоносные документы Word и файлы, замаскированные под PDF-документы. Примечательно, что помимо финальной вредоносной нагрузки — бэкдора — одна из жертв была заражена кастомной программой-вымогателем, что добавляет новую грань кампании Andariel: в одной из

предыдущих операций, связанной со взломом банкоматов, атакующие также стремились к получению финансовой выгоды.

Одновременно с нашим исследованием компания Malwarebytes опубликовала [отчет](#) с техническими подробностями этой серии атак, которые в отчете приписаны группе Lazarus. Однако после тщательного анализа эксперты «Лаборатории Касперского» пришли к более точной атрибуции атак: мы считаем, что за ними стояла группа Andariel — ответвление Lazarus. Данная атрибуция основана на совпадениях между кодом вредоносной нагрузки второго этапа из этой кампании и более раннего вредоносного ПО группы Andariel. Помимо сходства кода и аналогичного выбора жертв, использование команд Windows и их параметров в шелле-бэkdоре, применяемом после компрометации жертвы, было практически таким же, что и в более ранних кампаниях Andariel.

Группы, связанные с Китаем

Группа исследователей Cybereason Nocturnus Team [обнаружила](#) предназначенные для направленного фишинга вредоносные RTF-документы, созданные с помощью инструмента RoyalRoad и доставляющие PortDoor — не описанный ранее бэkdор, который, как считается, создан группой, действующей в интересах государства Китая. За несколько лет инструмент для создания вредоносных документов RoyalRoad, известный также под названием 8.t Dropper/RTF exploit builder, был включен в арсенал нескольких связанных с Китаем групп злоумышленников, включая Tick, Tonto Team и TA428. Все они регулярно пользуются RoyalRoad при проведении целевых фишинговых рассылок в рамках целенаправленных атак на значимые цели.

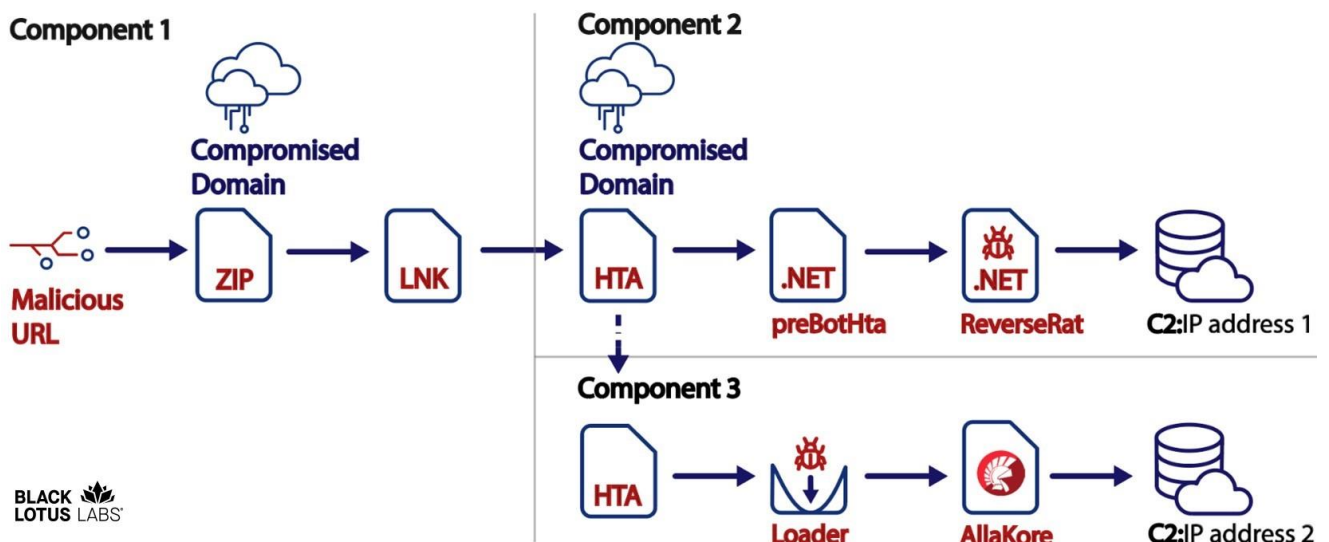
Исходя из анализа содержимого документа-приманки, мишенью атаки был генеральный директор конструкторского бюро «Рубин» — российского военного подрядчика, который проектирует подводные лодки для российского ВМФ.

В апреле и мае 2020 года организации на Тайване подверглись атакам программ-вымогателей, цель которых осталась неясной. В число атакованных организаций входят государственная нефтегазовая компания [CPC Corporation](#) — крупнейший поставщик бензина на Тайване, [Formosa Petrochemical Corporation](#), [Chunghwa Telecom](#) и, по сообщениям, организации из [полупроводниковой](#) отрасли. Учитывая целенаправленный характер этих атак, отсутствие сложных технических решений, отсутствие контактной информации для выплаты выкупа в некоторых вариантах программ-вымогателей, а также тот факт, что кампания была запущена всего за неделю до вступления в должность президента Тайваня, некоторые

считают, что реальной целью данных атак была не финансовая выгода, а что-то другое — например, нарушение нормальной работы компаний-жертв или отвлечение внимания от другой активности. 15 мая Бюро расследований Министерства юстиции (Investigation Bureau of the Ministry of Justice, MJIB) опубликовало [отчет](#) о расследовании, согласно которому за атаками стояла группа Winnti или другая тесно связанная с ней группа.

Атаки ReverseRat в Индии и Афганистане

Подразделение Black Lotus Labs компании Lumen [обнаружило](#) атаку с применением троянской программы для удаленного доступа ReverseRat. Большинство жертв атаки находятся в Индии, незначительная часть — в Афганистане. Среди жертв — государственная организация, организация по передаче электроэнергии и организация по производству и передаче электроэнергии где-то в «Южной и Центральной Азии» (страна не раскрывается). Операционная инфраструктура группировки, стоящей за этой кампанией, размещена в Пакистане, и исследователи предполагают, что сам актер также происходит из этой страны. Схема заражения, применяемая в рамках данной кампании, и ее тактики, методы и процедуры (TTP) аналогичны примененным в прошлогодней кампании, получившей название [Operation SideCopy](#).



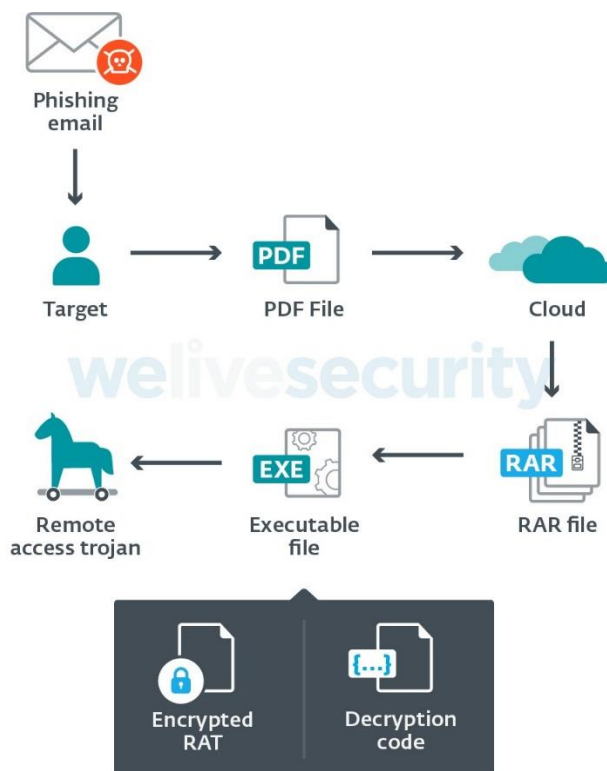
Многоступенчатый процесс заражения, наблюдаемый в ходе кампании
(Источник: [Lumen's Black Lotus Labs](#))

В результате многоступенчатой цепочки заражений на компьютер жертвы загружаются два агентских модуля: один (ReverseRAT) находится резидентно в оперативной памяти, а другой ([AllaKore](#)) загружается вместе с легитимной программой (side-loaded), позволяя злоумышленникам

закрепиться на зараженных рабочих станциях. Исходные URL-ссылки, с которых начинается цепочка заражений, не найдены, но, вероятно, их отправляли в специально созданных электронных письмах или сообщениях, как в других известных кампаниях данного актора.

Operation Spalax

Исследователи [обнаружили](#) атаки на колумбийские организации, включая государственные учреждения и частные компании, прежде всего в энергетической и металлургической отраслях. Эта серия атак, которая продолжается до сих пор, получила название "Operation Spalax". В ходе атак устанавливаются троянцы удаленного доступа — вероятнее всего, с целью ведения кибер-шпионажа.



Operation Spalax: схема заражения (Источник: [ESET](#))

Некоторые из тактик, методов и процедур, использованных в атаках, которые эксперты наблюдали в 2020 году, совпадают с описанными в более ранних отчетах о группах, специализирующихся на атаках на цели в Колумбии, — таких как [отчет QiAnXin](#) и [отчет TrendMicro](#). В атаке используются фишинговые письма, ведущие к загрузке вредоносных файлов. В большинстве случаев эти письма имеют во вложении PDF-документ, содержащий ссылку, по которой пользователь должен пройти для загрузки

вредоносного ПО. Загружаемые файлы — это обычные RAR-архивы, содержащие исполняемый файл. Модули вредоносной нагрузки, устанавливаемые в рамках операции Spalax, представляют собой популярные среди киберпреступников троянские программы удаленного доступа (RAT): Remcos, njRAT и AsyncRAT. Было обнаружено несколько дропперов, представляющих собой разные варианты упаковщика, использующего стеганографию и ранее примененного в образцах Agent Tesla. При этом вредоносная нагрузка Agent Tesla в этих дропперах отсутствовала.

Новые примеры активности Lazarus

В продолжение [расследования](#) атак группы Lazarus на предприятия оборонной промышленности с помощью вредоносного ПО ThreatNeedle эксперты «Лаборатории Касперского» [обнаружили](#) еще один кластер вредоносного ПО, который был назван CookieTime. Он используется в кампании, нацеленной на предприятия оборонной промышленности. Мы обнаруживали активность, связанную с этим кластером, в сентябре и ноябре 2020 года; при этом образцы вредоносного ПО датировались апрелем 2020 года. В сравнении с уже известными кластерами вредоносного ПО группы Lazarus у CookieTime иные структура и функциональность. Данное вредоносное ПО взаимодействует с командным сервером по протоколу HTTP. В ходе взаимодействия с командным сервером вредоносное ПО отправляет запросы в виде закодированных значений cookie и забирает командные файлы с сервера. Во взаимодействии с командным сервером используются методы стеганографии при обмене файлами между зараженными клиентскими компьютерами и командным сервером. Пересылаемые данные имеют вид файлов изображений в формате GIF, но при этом содержат зашифрованные команды, получаемые с командного сервера, и результаты выполнения команд. В результате тесного сотрудничества с местным центром CERT по отключению инфраструктуры группы злоумышленников исследователи «Лаборатории Касперского» получили возможность просмотреть выполняемый на командном сервере скрипт. Конфигурация командных серверов вредоносного ПО предусматривает проведение атак в несколько этапов, причем командный файл доставляется только на представляющие ценность хосты.

Исследователи ESET [обнаружили](#) не описанный ранее бэкдор, получивший название "Vuvuva". С его помощью была атакована компания по логистике грузоперевозок в Южной Африке. Бэкдор предназначен для сбора информации с компьютера жертвы и вывода собранных данных. Вредоносная программа взаимодействует с командным сервером через

сеть Tor. Исследователи приписывают эту активность группе Lazarus на основе общих черт с прошлой активностью и образцами вредоносного ПО этой группы.

RedEcho/ShadowPad

Исследователи компании Recorded Future с начала 2020 года [наблюдают](#) рост активности, связанной с целенаправленными вторжениями в системы предприятий электроэнергетики Индии. Они приписывают эту активность группе “RedEcho”. С середины 2020 года резко возросла интенсивность использования инфраструктуры, отслеживаемой Recorded Future как “AXIOMATICASYMPTOTE” и охватывающей командные серверы [ShadowPad](#).

Эксперты «Лаборатория Касперского» также исследовали атаки 2020–2021 годов в Индии, в которых использовались загрузчик ShadowPad и инфраструктура, описанная Recorded Future. На основе данных телеметрии было обнаружено более широкое географическое распределение жертв, среди которых есть объекты критической инфраструктуры. Инструментарий злоумышленников, включающий примененный в этих атаках обновленный загрузчик ShadowPad, получивший название “ShadowShredder”, описан в приватном отчете об АPT-атаках. Однако атрибуция этих атак по-прежнему под вопросом, поскольку вначале вредоносное ПО ShadowPad считалось частью арсенала [группы](#) BARIUM/APT41 (она же “Winnti”), но известно, что начиная с 2019 года оно применялось еще несколькими китайскоязычными АPT-группировками, такими как Tick, CactusPete, IceFog.

Zebrocy

В марте исследователи [обнаружили](#) кластер активности, связанной с атаками на Казахстан с применением Delphocy — вредоносного ПО, написанного на Delphi, которое ранее связывали с группой Zebrocy, считающейся подгруппой Sofacy. В качестве приманок использовались документы Word, якобы созданные в компании Казхром — одной из крупнейших в мире горно-металлургических компаний по добыче хромовой руды и производству ферросплавов. Всего было найдено шесть используемых Delphocy документов Word, которые, по-видимому, связаны с этим кластером. Все документы содержат один и тот же VBA-скрипт, доставляющий исполняемый файл в формате PE. Два из шести найденных документов, по-видимому, были загружены в сервис VirusTotal реальными жертвами атак из Казахстана.

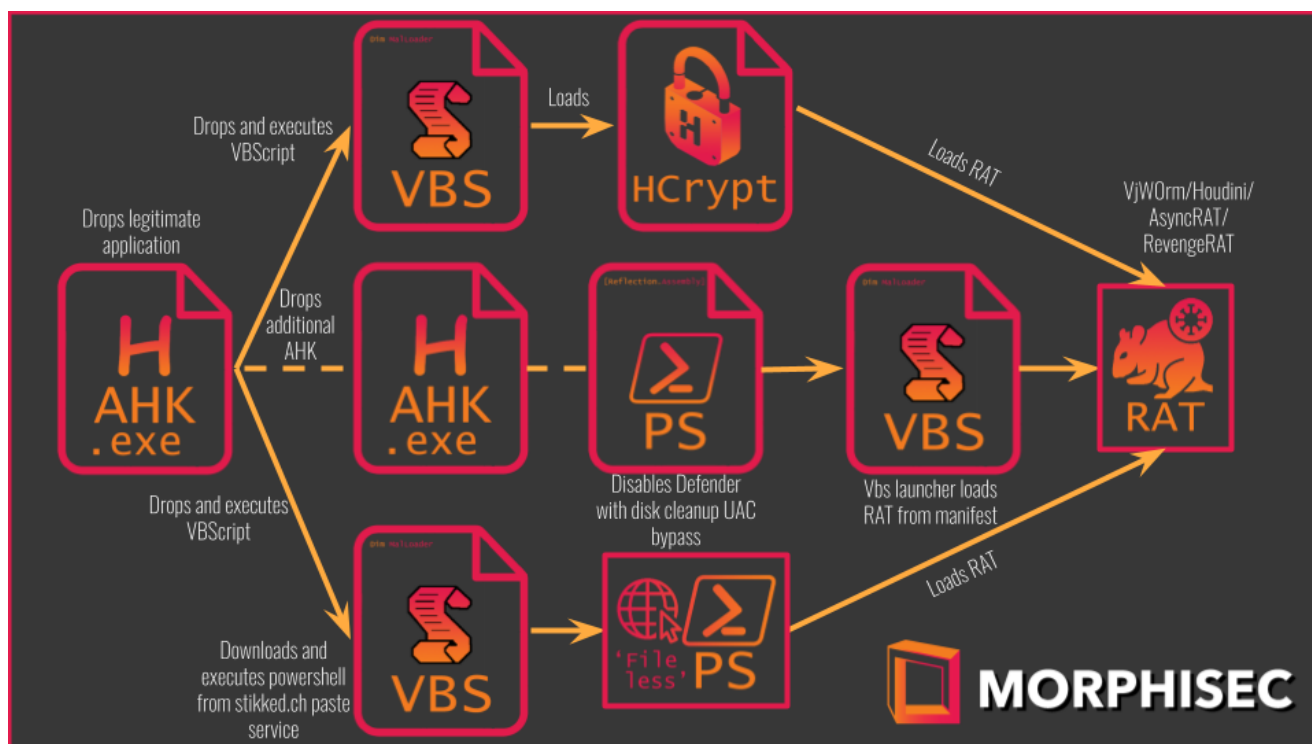
[Известно](#), что группировка Zebrocy еще в 2018 году атаковала промышленные компании Казахстана с применением документов, содержащих VBA-скрипты. Похоже, ее тактика осталась неизменной.

Атака на иранские центрифуги

10 апреля произошел [сбой электроснабжения](#) на иранском ядерном объекте в Нетензе, который затронул не только основное электрораспределительное оборудование, но и резервные системы. Вначале иранские официальные лица отказались подтвердить информацию о наличии жертв и ущербе, нанесенном оборудованию. Однако позднее власти подтвердили факт повреждения части центрифуг и признали, что «небольшой взрыв» «повредил секторы, [которые] могут быть оперативно отремонтированы». МИД Ирана [обвинил Израиль](#) в попытке вывести из строя главное иранское предприятие по обогащению урана, однако подтверждение этих обвинений отсутствует.

Атаки на аэрокосмическую отрасль с использованием утилит удаленного доступа (RAT)

Исследователи [сообщили](#) о продолжающейся фишинговой кампании, нацеленной на [организации аэрокосмической и туристической отраслей](#) и использующей новый загрузчик для скрытного развертывания различных вредоносных утилит удаленного доступа (RAT), таких как LimeRAT, RevengeRAT, AsyncRAT. Злоумышленники заманивают жертв с помощью изображений, замаскированных под PDF-документы с информацией, актуальной для отрасли, в которой работает потенциальная жертва.



Процесс заражения RAT (источник: [Morphisec](#))

Злоумышленники применяют троянские программы удаленного доступа для кражи данных, активности, связанной с дальнейшим развитием атаки, и доставки дополнительной вредоносной нагрузки, включая троянца Agent Tesla, которого они используют для вывода украденных данных. Загрузчик активно развивается. Компания Morphisec дала ему имя [Snip3](#).

Gelsemium

APT-группа Gelsemium, ориентированная на кибершпионаж и активно действующая с 2014 года, [считается](#) ответственной за недавние атаки на цепочки поставок организаций в Китае, Японии, Монголии, на Тайване, в Северной и Южной Корее и нескольких странах Ближнего Востока. Среди мишеней атак — государственные органы, религиозные организации, производители электроники и университеты. Впервые данная атака на цепочки поставок была описана в статье исследователей компании ESET [Operation NightScout](#). Злоумышленники взломали механизм обновления NoxPlayer — эмулятора Android для компьютеров Windows и Mac, входящего в продуктовую линейку компании BigNox, у которой более 150 миллионов пользователей по всему миру. При анализе кампаний Gelsemium исследователи ESET обнаружили новую версию сложного модульного

вредоносного ПО Gelsemium, а также дополнительные инструменты, такие как бэкдоры OwlProxy и Chrommme.

Заключение

Что же наиболее важного можно вынести, проанализировав публично доступную информацию об АРТ-атаках на промышленные организации в первом полугодии 2021 года?

В первую очередь — что порчи продукции, вывода из строя оборудования и прочих (включая даже более тяжёлые) физических последствий атак на системы технологических сетей предприятий исследователями АРТ выявлено не было. В этой связи стоит упомянуть инцидент на станции водоочистки во Флориде, но с большой вероятностью ни одна из АРТ к нему причастна не была, поэтому в этот отчёт мы его не включили. Что же касается происшествия на предприятии в Нетензе, то никаких надёжных данных, указывающих на кибер-природу вызвавших его событий, в публичных источниках нам найти не удалось.

Следующие по важности выводы, на наш взгляд, отражают общие тенденции развития современного ландшафта угроз для организаций различных секторов, типов и профилей и подсвечивают общие проблемы, стоящие как перед сообществом исследователей угроз, так и перед экспертами в практической киберзащите ИТ- и ОТ-инфраструктур.

Мы можем констатировать, что:

1. Всё чаще приходится наблюдать в арсенале АРТ-групп инструментарий, который раньше ассоциировался преимущественно с криминальными атаками.
 - Социальная инженерия остается наиболее популярным способом начального проникновения не только для киберкриминала, но и для АРТ.
 - АРТ группы часто не утруждают себя попытками использовать уязвимости нулевого дня — ведь инфраструктура их потенциальных жертв полна старых, хорошо известных и уже используемых другими злоумышленниками уязвимостей (пример — атаки с эксплуатацией уязвимостей SSL-VPN-шлюзов).
 - Широкое применение коммерческого вредоносного ПО теперь не указывает на сугубо криминальную природу атаки.
 - Использование в атаке уязвимости нулевого дня перестало быть чётким признаком АРТ.

2. Популярность «коммерческого» вредоносного ПО в арсеналах АРТ можно объяснить не только чисто экономическими соображениями, но и логичным желанием остаться незамеченным или хотя бы неузнанным, затерявшись среди гигантского количества криминальных атак.
3. Впрочем, с этой же целью у киберкриминала можно заимствовать не только инструментарий, но и инфраструктуру (об этом мы расскажем в наших следующих публикациях) и даже стратегию. В первом полугодии (как мы и [предсказывали](#)) АРТ группа вслед за операторами ExPetr пыталась маскировать свою активность под атаки ransomware.
4. Классификация различного инструментария и используемой в атаках инфраструктуры в попытке разобраться, кто же стоит за атакой (которую стало принято в кругах специалистов по ИБ называть «атрибуцией»), и составить энциклопедию известных групп, продолжает оставаться сложной задачей. Несмотря на большой объём работы, проделанной в этом направлении множеством исследователей, к консенсусу часто прийти не удаётся. Профессиональные киберзлоумышленники оставляют не много следов, и распутать их преступления в виртуальном мире «без санкции прокурора» бывает невозможно. Исследования серии нашумевших атак, связанных с SolarWinds, замечательно это демонстрируют.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com