

Атаки на промышленные предприятия с использованием RMS и TeamViewer: новые данные

Вячеслав Копейцев

Содержание

Содержание	1
Краткое содержание отчета	2
Технический анализ	2
Распространение	2
Особенности вредоносного ПО	4
Инфраструктура	8
Жертвы	9
Атрибуция	9
Заключение	10
Рекомендации	11
Приложение I – Индикаторы компрометации	12
Приложение II – Описание атаки по MITRE ATT&CK	14

Летом 2019 года Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) зафиксировал очередную волну рассылок фишинговых писем, содержащих различные вредоносные вложения. Рассылки нацелены на компании и организации из разных секторов экономики, деятельность которых так или иначе связана с промышленным производством.

Об этих атаках мы уже сообщали в 2018 году в статье [“Атаки на промышленные предприятия с использованием RMS и TeamViewer”](#), однако последние полученные данные позволяют говорить о том, что злоумышленники модифицировали методы атак, а также о том, что угрозе заражения подвергается всё больше предприятий.

Мы публикуем данный отчёт, дождавшись, когда производитель ПО RMS внёс изменения в работу своих сервисов, чтобы результаты данного исследования не могли быть использованы в целях эксплуатации уязвимостей.

Краткое содержание отчета

- С 2018 года и как минимум до осени 2020 года злоумышленники рассылали фишинговые письма, содержащие вредоносное ПО.
- В атаках используются приемы социальной инженерии и легитимные документы, такие как служебные записки и документы с настройками оборудования или другой информацией о технологическом процессе, которые, по-видимому, были украдены у атакуемой компании или её деловых партнеров.
- В атаках по-прежнему используются утилиты удаленного администрирования, графический интерфейс которых скрывается вредоносным ПО, что позволяет злоумышленникам скрыто управлять зараженной системой.
- В новой версии вредоносного ПО злоумышленники изменили канал оповещения о заражении новых систем: вместо серверов управления вредоносным ПО используется веб-интерфейс облачной инфраструктуры управления утилиты удаленного администрирования RMS.
- Основной целью злоумышленников по-прежнему является кража денежных средств атакуемой организации.
- В ходе проведения атаки преступники используют шпионское ПО (spyware) и утилиту Mimikatz для кражи аутентификационных данных, которые потом используются для заражения других систем внутри сети предприятия.

Полная версия статьи доступна на [Kaspersky Threat Intelligence](#).

За дополнительной информацией вы можете обратиться по адресу: ics-cert@kaspersky.com

Технический анализ

Мы уже подробно описывали технические детали этой серии атак в предыдущем отчёте “[Атаки на промышленные предприятия с использованием RMS и TeamViewer](#)”, поэтому в данном документе лишь напомним основные этапы атаки и опишем изменения в тактике и инструментарии злоумышленников, произошедшие со времени выхода предыдущего отчета.

Распространение

Фишинговые письма, используемые в данной атаке, чаще всего замаскированы под деловую переписку между организациями. В частности, рассылаются претензионные письма от имени крупной промышленной компании.



Дмитриев Петр Васильевич <[REDACTED]>

Запрос № 6430787 от [REDACTED]

Кому [REDACTED]



Перечень документов.rar
143 Б

Здравствуйте, прошу ознакомиться с претензионно-информационным письмом для Вашего предприятия, с целью конфиденциальной переписки прошу использовать для вложений пароль. В приложение высылаю запрос от ОАО «[REDACTED]» на ваше имя, пароль 25262

Просьба ответить на запрос

*** Настоящее сообщение (включая любые приложения к нему) предназначено только для указанного в нем адресата. Если данное сообщение попало к Вам по ошибке, пожалуйста, незамедлительно проинформируйте об этом его отправителя, а само сообщение уничтожьте. Настоящим Вам также сообщается, что любое несанкционированное раскрытие, копирование или распространение данного сообщения или совершение каких-либо действий, основанных на информации, содержащейся в нем, строго запрещено. Содержащиеся в сообщении утверждения не являются официальной позицией ОАО «[REDACTED]», если иное прямо не указано отправителем.

Пример фишингового письма, замаскированного под претензионное письмо

В предыдущей серии атак в адресе электронной почты отправителя письма злоумышленники использовали доменное имя, схожее с адресом официального сайта организации, от имени которой было отправлено фишинговое письмо. Теперь для отправки писем используются публичные почтовые сервисы. Чтобы ввести в заблуждение получателя письма и убедить его открыть вредоносное вложение, злоумышленники применяют другую технику: они представляются реальным деловым партнером или представителем реально существующей дочерней организации атакуемой компании и просят ознакомиться с предоставленными документами не позднее обозначенного в письме срока, мотивируя это окончанием конкурса на закупку, наступлением штрафных санкций или необходимостью срочного ознакомления с данными о настройках оборудования.

Также стоит обратить особое внимание на то, что фишинговые письма формируются индивидуально для каждой из атакуемых компаний. Об этом говорит упоминание атакуемой компании в тексте письма, а также документы, используемые в атаках злоумышленниками (данные документы будут описаны ниже). В некоторых случаях, зафиксированных ранее, злоумышленники также обращались к получателю письма по фамилии, имени и отчеству.

Message | Документы на поставку.rar (3 MB)

From: АО «[REDACTED]» [mailto:info@[REDACTED]]
Sent: [REDACTED]
To: [REDACTED]
Subject: ищ: 55346

Здравствуйте компания «[REDACTED]» являясь комплексным поставщиком оборудования компании ПАО «[REDACTED]» и дочерних обществ, в настоящее время проводится процедура заключения договора на поставку Вашего оборудования и дополнительных услуг. Ваша организация выбрана поставщиком по лоту [REDACTED] на сумму [REDACTED],000 руб. Прошу ознакомиться со спецификацией на ваше оборудование, в случае замечаний прошу внести корректировку и отправить нам в обратный адрес!

Предложения принимаются в срок до 12.00 [REDACTED]. Обращаю внимание Участников в первую очередь высылается Заявка участника с подписанной формой для заполнения (спецификация) + Форма 1 в ответ на это письмо, после все указанные документы по дополнительному запросу.

Организация вправе принять решение по разделению лота на отдельные закупки.

По всем вопросам прошу звонить /или писать

В целях обеспечения конфиденциальности на всех документах установлен пароль 9887676.

--

Спасибо за оперативность!

И.о. Начальник управления

подготовки конкурсных

процедур [REDACTED]

тел.: [REDACTED]

info@[REDACTED]

Пример фишингового письма, отправленного от имени подрядчика

В качестве вложений к фишинговым письмам прикреплены архивы, защищенные паролем, указанным в тексте письма. В теле письма злоумышленники обосновывают такой способ передачи информации соображениями конфиденциальности, однако использование пароля позволяет предотвратить сканирование антивирусными средствами файлов, находящихся в архиве.

Особенности вредоносного ПО

Внутри архива, прикрепленного к письму, находятся несколько вредоносных обфусцированных JS-скриптов, имеющих идентичную функциональность, но немного разную структуру из-за применения различных техник обфускации кода. Имена скриптов, как правило, замаскированы под названия документов.

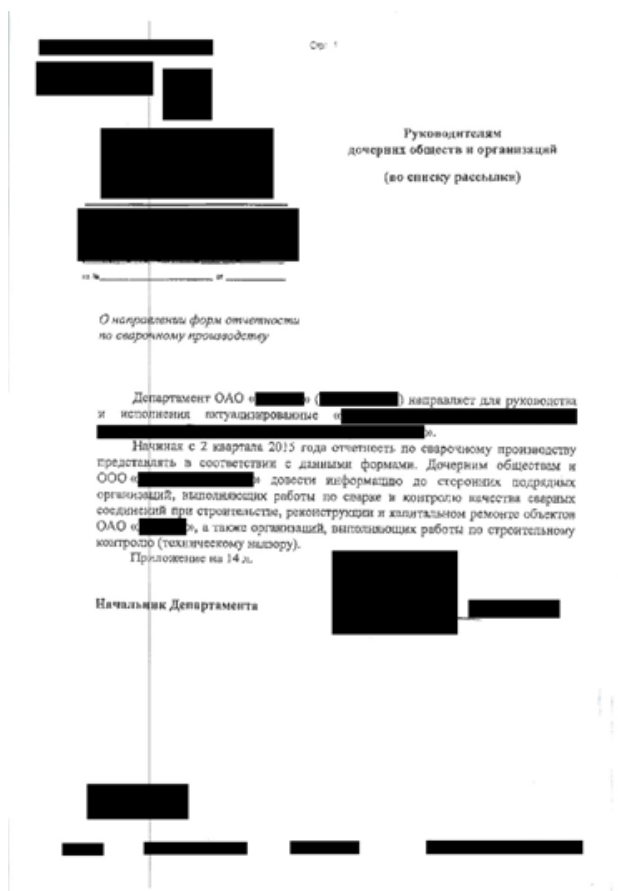
Запуск такого скрипта пользователем приведёт к распаковке и открытию двух файлов: вредоносной программы, детектируемой как HEUR:Backdoor.Win32.Generic, и легитимного PDF-файла. Некоторые обнаруженные варианты JS-скриптов загружают указанные файлы с удаленного сервера, а не извлекают из тела скрипта.

В предыдущих атаках, чтобы у пользователя не возникло вопросов по поводу отсутствия документов, о которых говорилось в тексте письма, а также для того, чтобы отвлечь его внимание во время установки вредоносного ПО, злоумышленники открывали поврежденный PDF-документ или изображение, либо запускали инсталлятор легитимного ПО.



Изображение, открываемое вредоносной программой в предыдущих атаках

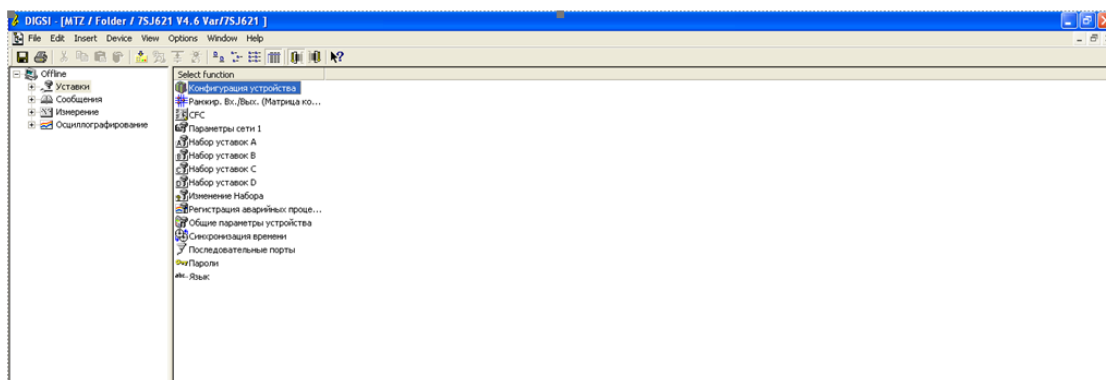
В более поздних атаках злоумышленники начали использовать рабочие документы, связанные со спецификой деятельности атакуемой организации. Документ может выглядеть как принадлежащий деловому партнеру или даже самой атакованной организации. В частности, были использованы скан-копии служебных записок, писем к дочерним и подрядным организациям, а также формы закупочной документации, которые, по-видимому, были украдены ранее.



Пример PDF документа с распоряжением для дочерних предприятий, который использовали злоумышленники

Особенно интересен тот факт, что в некоторых случаях были использованы документы, содержащие информацию о настройках промышленного оборудования, а также о других параметрах технологического процесса.

В частности, использованы скриншоты из приложения DIGSI. Это приложение является конфигуратором устройств релейной защиты и автоматики (РЗА) производства Siemens.



Скриншот ПО DIGSI №1

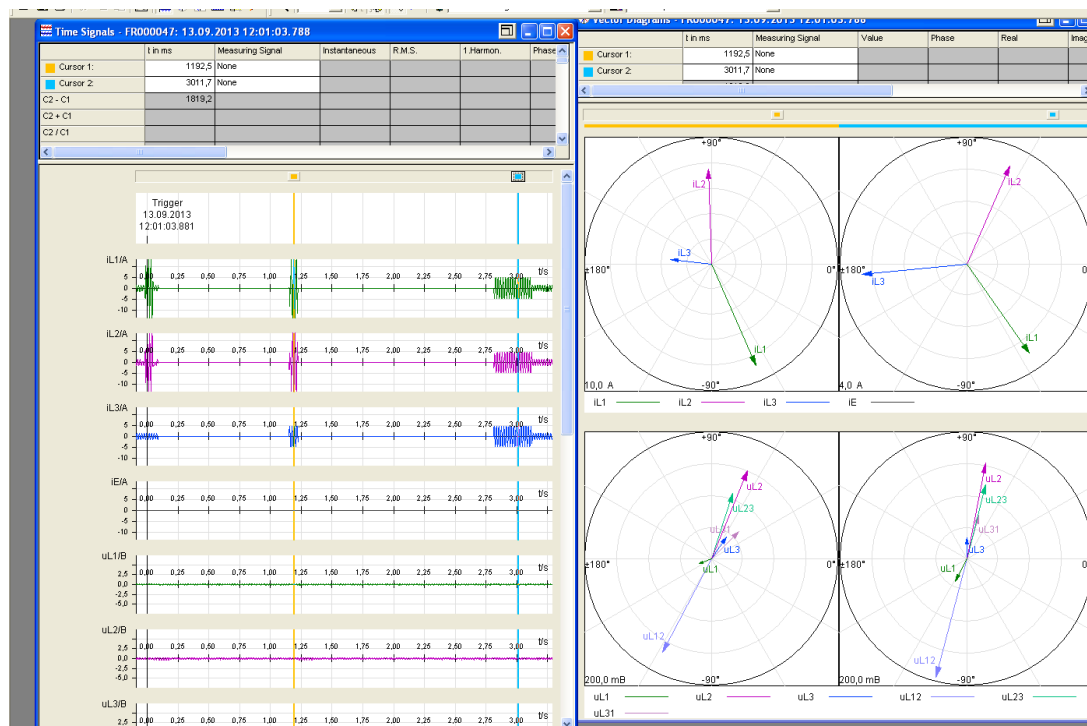
DIGSI используется для настройки систем релейно-защитной автоматики на объектах электроэнергетики, в частности, на подстанциях.

Power System Data 1		
Power System Transformer CT's Breaker		
Settings:		
No.	Settings	Value
0201	CT-Strpnt. Side1 in Direct. of Object	NO
0202	CT Rated Primary Current Side 1	100 A
0203	CT Rated Secondary Current Side 1	5A
0206	CT-Strpnt. Side2 in Direct. of Object	YES
0207	CT Rated Primary Current Side 2	200 A
0208	CT Rated Secondary Current Side 2	5A
0230	Grounded Electrode versus	Terminal Q7
0232	CT Rated Primary Current I7	200 A
0233	CT Rated Secondary Current I7	5A
0235	Factor: Prim. Current over Sek. Curr. I8	60,0

Скриншот ПО DIGSI №2

Скриншот матрицы конфигурации РЗА. Список уставок

Также в документах, использовавшихся злоумышленниками, мы обнаружили скриншоты с осциллограммами трансформаторов:



Скриншот векторных диаграмм с осциллограммами

Стоит отметить, что на последнем скриншоте приведены осциллограммы системы в момент аварии.

Фишинговые письма с такими скриншотами не содержат призывов к установке настроек, приведённых в документах. Наиболее вероятно, что документы с показанными скриншотами используются злоумышленниками в целях отвлечения внимания персонала на время установки вредоносного ПО. Специалисту по РЗА все эти данные могут дать представление о том, какие типовые настройки установлены на объекте, поэтому сам факт наличия таких скриншотов у злоумышленников вызывает опасения.

Далее JS-скрипт запускает вредоносную программу, которая устанавливает в систему модифицированное злоумышленниками средство удаленного администрирования (Remote Administration Tool – RAT) TeamViewer. Как и в предыдущих атаках, злоумышленники используют вредоносную DLL-библиотеку для сокрытия графического интерфейса, чтобы без ведома пользователя управлять зараженной системой.

При необходимости сбора дополнительных сведений злоумышленники загружают дополнительный набор вредоносного ПО, сформированный индивидуально для каждой жертвы. Это может быть шпионское вредоносное ПО (класс Spyware), позволяющее собирать логины и пароли от множества различных программ и сервисов – почтовых клиентов, браузеров, SSH/FTP/Telnet клиентов, а также регистрировать нажатия клавиш и делать снимки экрана. В некоторых случаях применяется утилита Mimikatz, позволяющая получить данные аккаунтов учетных записей Windows, ранее введенных на скомпрометированной системе. Использование утилиты Mimikatz особенно опасно, поскольку может позволить злоумышленникам получить доступ сразу к большому количеству систем в сети предприятия.

В большинстве случаев для сокрытия следов вредоносной активности в системе злоумышленники маскируют компоненты вредоносного ПО под компоненты операционной системы Windows.

Инфраструктура

В ходе анализа новой серии атак мы заметили два отличия с точки зрения организации инфраструктуры.

Во-первых, для размещения файлов, которые скачиваются вредоносными JS-скриптами на этапе заражения системы, злоумышленники используют ресурсы, замаскированные под веб-сайты различных реально существующих русскоязычных компаний.

Второе и более важное отличие заключается в том, что злоумышленники исключили из схемы коммуникаций с зараженными системами сервер управления вредоносным ПО.

Основной причиной существования сервера управления вредоносным ПО в данной схеме атаки являлась необходимость получить ID зараженной машины в системе TeamViewer, т.к. всю другую необходимую информацию злоумышленники уже знали (пароль, необходимый для подключения, был задан в специальном конфигурационном файле). В новой серии атак для передачи идентификатора машины в системе TeamViewer была использована легитимная инфраструктура утилиты удаленного администрирования RMS.

Дело в том, что облачная инфраструктура удаленного администрирования RMS имеет специальный веб-сервис, позволяющий уведомлять администратора о том, что дистрибутив RMS был установлен на удаленной системе. При этом сервером RMS генерируется сообщение электронной почты, содержащее в тексте письма ID машины в системе RMS. Для этого клиентской части RMS достаточно выполнить HTTP POST запрос на специальную веб-страницу и передать имя продукта, ID языкового пакета системы, имя пользователя, имя компьютера, адрес электронной почты, на который необходимо доставить уведомление, а также ID машины в системе RMS, который был присвоен после установки программы.

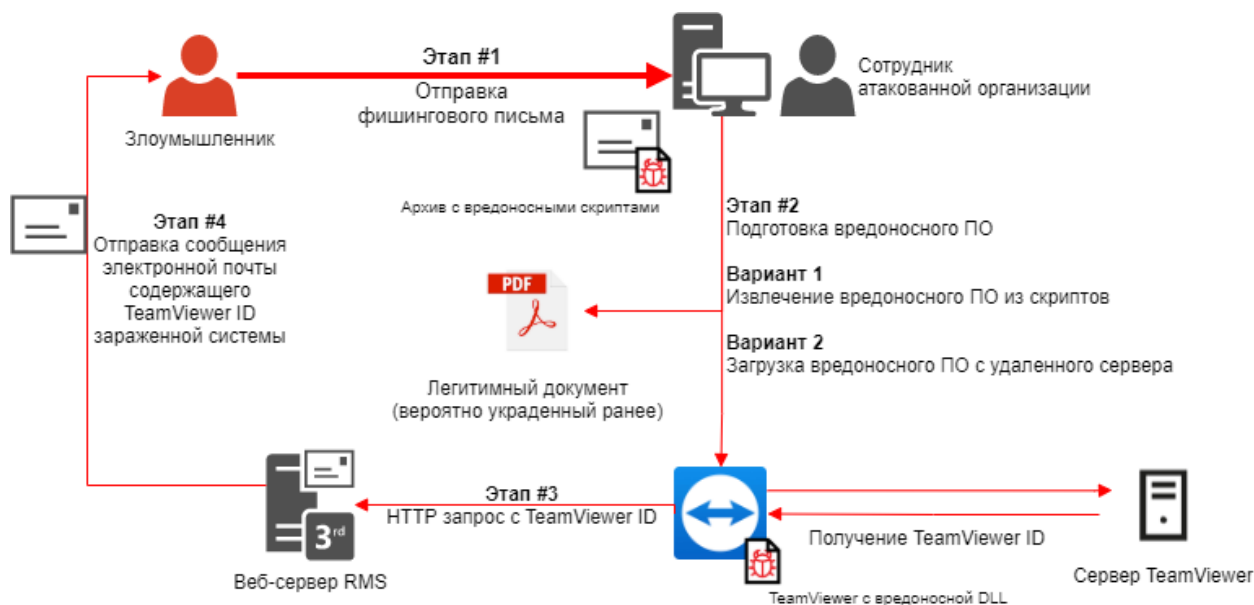


Схема проведения атаки

Механизм работы данного веб-сервиса содержал уязвимость, которая заключается в отсутствии какой-либо процедуры авторизации. Вредоносная DLL, которая занимается сокрытием графического интерфейса TeamViewer, содержала код отправки соответствующего запроса на сервер RMS. Только вместо ID машины в системе RMS

отправлялся ID машины в системе TeamViewer. Длина ID в системе TeamViewer отличается от длины ID в системе RMS, однако отсутствие проверки содержимого полей, передаваемых на сервер в HTTP POST запросе, позволяло успешно сформировать и доставить сообщение с уведомлением о зараженной машине на адрес злоумышленника.

Kaspersky ICS CERT уведомил разработчиков RMS о факте использования их инфраструктуры в преступных целях и передал все технические подробности, необходимые для устранения уязвимости. На данный момент описанная выше уязвимость не была устранена разработчиками, однако было реализовано обходное решение – фильтрация по белому списку адресов.

Иначе говоря, описанная функциональность до сих пор работает, однако письма с уведомлениями отправляются только на адреса электронной почты, находящиеся в специальном списке клиентов, «проверенных» разработчиками RMS.

Для получения технической информации о данной уязвимости вы можете обратиться по адресу: ics-cert@kaspersky.com

Жертвы

Как уже было сказано, подавляющее большинство атакованных систем составляют промышленные предприятия из России, представляющие различные секторы экономики. Нами были зафиксированы атаки на компании из следующих индустрий:

- Производство
- Нефть и газ
- Металлургия
- Инжиниринг
- Энергетика
- Строительство
- Добыча полезных ископаемых
- Логистика

Исходя из этого, нельзя говорить об узкой направленности атаки на одну конкретную индустрию, однако тот факт, что большинство легитимных документов, использованных в атаках, относятся к энергетике, позволяет предположить, что злоумышленники проявляют повышенный интерес к этой отрасли.

Атрибуция

Мы уверены, что за атаками стоит русскоговорящая группировка.

Основные аргументы в пользу этого предположения были изложены в нашем предыдущем отчете "[Атаки на промышленные предприятия с использованием RMS и TeamViewer](#)".

В дополнение к ранее изложенной информации заметим, что код обращения к серверу RMS, обнаруженный в ходе анализа новой версии вредоносной DLL, содержит ID языка, обозначающего русскую локализацию операционной системы.

Согласно имеющейся информации основной целью преступников является кража денежных средств со счетов организаций. Это означает, что злоумышленникам необходимо хорошо ориентироваться в организации финансовых процессов, которые имеют специфические особенности в каждой стране, в том числе поддерживать соответствующую инфраструктуру для вывода денежных средств.

Группировка не использует сложных тактик или технических средств, однако тщательно готовит каждую из атак и умело использует приемы социальной инженерии, а также технические средства, уже известные ранее по атакам других преступных группировок.

В состав группы предположительно входят люди, ответственные за техническую часть заражения систем, а также люди, ответственные за финансовые операции, т.е. непосредственно за кражу денежных средств.

Заключение

Злоумышленники продолжают успешно атаковать промышленные предприятия, используя довольно простые техники, однако их методы всё же эволюционируют. Для того чтобы убедить пользователя в легитимности фишинговых писем, преступники начали использовать документы, предположительно украденные во время предыдущих атак. Стоит отметить, что используются в том числе и документы с описанием настроек промышленного оборудования и параметров технологического процесса, что лишний раз подтверждает направленность атак на промышленные предприятия.

Основным техническим изменением в атаках стал отказ злоумышленников от наиболее уязвимого этапа сбора и передачи данных – серверов управления вредоносным ПО, которые могут быть отключены провайдером хостинга и заблокированы системами ИБ. Вместо этого для доставки сообщений о заражении систем используется легитимный веб-интерфейс облачной инфраструктуры утилиты удаленного администрирования RMS. Для хранения образцов вредоносного ПО использованы ресурсы, замаскированные под легитимные веб-сайты реально существующих организаций.

С момента заражения злоумышленники имеют возможность полного удаленного контроля над зараженной системой. Основной целью атакующих остается кража денежных средств со счетов организации. Когда злоумышленники подключаются к компьютеру жертвы, они ищут ПО для осуществления финансовых и бухгалтерских операций (1С бухгалтерия, банк-клиент и др.). Кроме того, они находят и изучают бухгалтерские документы о проводимых закупках, а также изучают почтовую переписку сотрудников предприятия. Далее злоумышленники ищут всевозможные способы для совершения финансовых махинаций. Мы предполагаем, что злоумышленники могут подменять реквизиты, по которым производится оплата счетов.

Несомненно, наличие у злоумышленников удаленного доступа к зараженным системам влечет и другие угрозы, такие как утечка конфиденциальных данных организации, выведение систем из строя и т.д. Как показали последние события, документы, вероятно украденные у организаций, используются злоумышленниками для проведения последующих атак, в том числе на партнеров пострадавших компаний.

Если вы столкнулись с подобной атакой, вы можете сообщить нам об этом через [форму](#) на нашем сайте.

Рекомендации

- Проводить обучение сотрудников предприятия безопасной работе с электронной почтой и, в частности, выявлению фишинговых сообщений.
- Ограничить возможность программ получать привилегии SeDebugPrivilege (там, где это возможно).
- Установить на всех системах антивирусное ПО с поддержкой централизованного управления политикой безопасности; поддерживать антивирусные базы и программные модули защитных решений в актуальном состоянии.
- Использовать учетные записи с привилегиями администратора домена только в случае необходимости. После использования таких учетных записей перезагрузить систему, на которой осуществлялась аутентификация.
- Внедрить парольную политику с требованиями к сложности паролей и их регулярной смене.
- В случае подозрений, что некоторые системы заражены: удалить все сторонние утилиты удаленного администрирования, выполнить проверку этих систем антивирусным ПО и обеспечить смену паролей для всех учетных записей, использованных для входа на скомпрометированных системах.
- Осуществлять мониторинг сетевых подключений с целью выявления следов работы утилит удаленного администрирования, установленных без надлежащих согласований. Особое внимание уделять фактам использования утилит RMS и TeamViewer.
- Используя решения для фильтрации сетевой активности, заблокировать возможность подключения к серверам и IP адресам, указанным в Приложении I – Индикаторы компрометации.
- Не использовать устаревшие версии утилиты TeamViewer (версий 6.0 и ниже). Для обнаружения фактов использования устаревших версий утилиты TeamViewer можно воспользоваться правилом YARA, представленным в Приложении I – Индикаторы компрометации
- Следует отметить, что, поскольку в атаке используется легитимное ПО для удаленного администрирования, даже после удаления вредоносного загрузчика данное ПО может остаться на компьютере жертвы и продолжить работать. Если на этапе проверки корпоративных систем обнаружено ПО для удаленного управления, в каждом случае необходимо определить, легитимно ли оно установлено.

За дополнительной информацией вы можете обратиться по адресу: ics-cert@kaspersky.com

Приложение I – Индикаторы компрометации

File Hashes (malicious documents, malware, emails etc.)

- 386a1594a0add346b8fbbefcf1547e77
- 203e341cf850d7a05e44fafc628aeaf1
- 3b79aacdc33593e8c8f560e4ab1c02c6
- ea1440202beb02cbb49b5bef1ec013c0
- 1091941264757dc7e3da0a086f69e4bb
- 72f206e3a281248a3d5ca0b2c5208f5f
- da4dff233ffbac362fee3ae08c4efa53
- d768a65335e6ca715ab5ceb487f6862f
- 9219e22809a1dff78aac5fff7c80933c
- 86e14db0bcf5654a01c1b000d75b0324

File Names

- Акт.js
- Запрос 17782-09-1.js
- Перечень документов.js
- спецификация на оборудование xls.js
- tv.dll
- tv.ini

Some malware modules installed on the system have randomly generated names that follow a specific format. The following regular expression can be used to search for such files:

```
%TEMP%\\[a-z]{2,3}[0-9]{2}.exe
```

These files are saved in the temporary file directory (%TEMP%); the first part of the file name consists of two or three Roman characters; the second is a two-digit number followed by the extension .exe

Domains and IPs

- timkasprot.temp.swtest[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)
- 77.222.56[.]169 (RemoteAdmin.Win32.RemoteManipulator.vpj)
- z-wavehome[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)
- dncars[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)

Yara Rules

```
rule TeamViewer_ver6_and_lower {
meta:
    description = "Rule to detect TeamViewer ver 6.0 and lower"
    hash = "4f926252e22afa85e5da7f83158db20f"
    hash = "8191265c6423773d0e60c88f6ecc0e38"
    version = "1.1"
```

condition:

```
uint16(0) == 0x5A4D and  
pe.version_info["CompanyName"] contains "TeamViewer" and  
(pe.version_info["ProductVersion"] contains "6.0" or  
pe.version_info["ProductVersion"] contains "5.1" or  
pe.version_info["ProductVersion"] contains "5.0" or  
pe.version_info["ProductVersion"] contains "4.1" or  
pe.version_info["ProductVersion"] contains "4.0" or  
pe.version_info["ProductVersion"] contains "3.6" or  
pe.version_info["ProductVersion"] contains "3.5" or  
pe.version_info["ProductVersion"] contains "3.4" or  
pe.version_info["ProductVersion"] contains "3.3" or  
pe.version_info["ProductVersion"] contains "3.2" or  
pe.version_info["ProductVersion"] contains "3.1" or  
pe.version_info["ProductVersion"] contains "3.0")
```

}

The attackers use outdated versions of the TeamViewer client that contain a vulnerability enabling them to hide the utility's graphic interface. This YARA rule can be used to determine whether there are outdated versions of the TeamViewer software installed on the system. Checking whether any such software found was installed legitimately is a first-priority task.

If instances of outdated versions of the TeamViewer client being used legitimately are identified, it is recommended that the software in question be updated to the latest version.

Registry keys

- Key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\rundll32
Value:
rundll32.exe shell32.dll,ShellExec_RunDLL
"%AppData%\Roaming\TeamViewer\5\TeamViewer.exe"
- Key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\CCFTray
Value:
rundll32.exe shell32.dll,ShellExec_RunDLL "%temp%\TeamViewer.exe"

Threat actors' email addresses

- timkas@protonmail.com
- smollsrv@gmail.com
- nataly@z-wavehome.ru
- info@dncars.ru

Приложение II – Описание атаки по MITRE ATT&CK

Тактика (Tactic)	Техники (Technique/Subtechnique)	Описание
Initial Access	T1566.001	Phishing: Spearphishing Attachment Злоумышленники используют фишинговые письма с архивами, содержащими вредоносные скрипты
Execution	T1204.002	User Execution: Malicious File Вредоносное ПО выполняется при открытии файла пользователем
	T1059.007	Command and Scripting Interpreter: JavaScript/Jscript Используется для открытия вредоносных исполняемых файлов (PE) и файлов-приманок PDF
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder Вредоносное ПО создаёт ключ реестра для автоматического запуска после перезагрузки системы
Defense Evasion	T1027.002	Obfuscated Files or Information: Software Packing Чтобы затруднить анализ, вредоносное ПО упаковано, а код обфусцирован
	T1564.001	Hide Artifacts: Hidden Files and Directories Вредоносным файлам назначаются атрибуты «скрытый» и «системный»
	T1574.001	Hijack Execution Flow: DLL Search Order Hijacking Чтобы скрыть пользовательский интерфейс утилиты удаленного администрирования TeamViewer, в процесс вместо системной библиотеки загружается модель вредоносной программы
	T1036.005	Masquerading: Match Legitimate Name or Location В большинстве случаев для сокрытия следов вредоносной активности в системе

		злоумышленники маскируют компоненты вредоносного ПО под компоненты операционной системы Windows
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory В случаях, когда злоумышленникам необходимы аутентификационные данные для заражения других систем, они используют утилиту Mimikatz
	T1056.001	Input Capture: Keylogging В некоторых случаях злоумышленники загружают на зараженную систему вредоносное ПО (класс Spyware), позволяющее собирать логины и пароли от множества различных программ и сервисов, регистрировать нажатия клавиш и делать снимки экрана
Discovery	T1057	Process Discovery Вредоносное ПО собирает информацию об антивирусных программах, работающих в системе
	T1018	Remote System Discovery Злоумышленники изучают другие системы организации, к которым они могут получить доступ по сети
	T1518	Software Discovery Злоумышленники отмечают, какое ПО, связанное с проведением финансовых операций, установлено на зараженных системах
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol Для заражения других систем предприятия используется подключение по RDP с применением учетных данных, полученных ранее с помощью утилиты Mimikatz
Collection	T1005	Data from Local System Злоумышленники изучают документы, обнаруженные на зараженных системах; эти документы могут использоваться в дальнейших атаках

	T1114.001	Email Collection: Local Email Collection Злоумышленники изучают деловую корреспонденцию атакуемой организации, чтобы использовать ее в последующих атаках на бизнес-партнеров жертвы
	T1056.001, T1113	Input Capture: Keylogging and Screen Capture В некоторых случаях на зараженную систему загружается вредоносное ПО (класс Spyware), позволяющее собирать логины и пароли от множества различных программ и сервисов, регистрировать нажатия клавиш и делать снимки экрана
Command And Control	T1071.001	Application Layer Protocol: Web Protocols Для отправки ID в системе TeamViewer на сервер RMS выполняется HTTP POST запрос
	T1071.003	Application Layer Protocol: Mail Protocols Сервер RMS посылает письмо на адрес электронной почты, контролируемый злоумышленниками. В письме содержится ID зараженной машины в системе TeamViewer
	T1219	Remote Access Software Для подключения к зараженной системе злоумышленники используют утилиту удаленного администрирования TeamViewer
Exfiltration	T1020	Automated Exfiltration Злоумышленники используют вредоносное ПО для получения информации, собранной на зараженной системе
Impact	T1565.001	Data Manipulation: Stored Data Manipulation Подмена банковских реквизитов в платежных формах

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