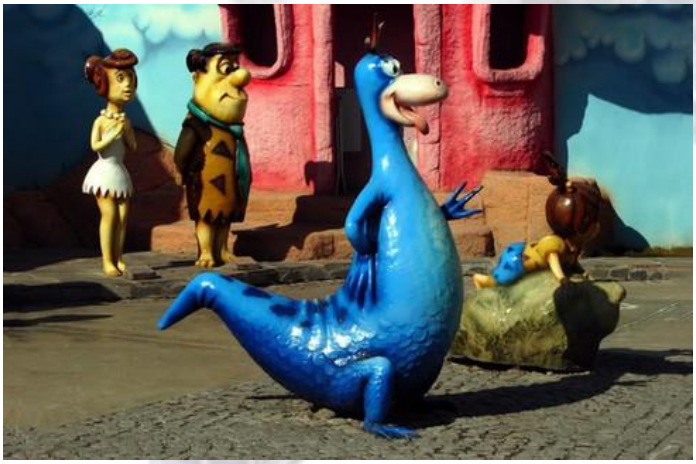
Dino – новое state-sponsored шпионское ПО с французскими корнями

В этом ресерче мы рассмотрим новое вредоносное ПО, которое его создатели назвали Dino. Dino представляет из себя сложный бэкдор, который был разработан кибергруппой Animal Fram, стоявшей за созданием и распространением такого state-sponsored вредоносного ПО как Casper, Bunny и Babar. Он содержит в себе много интересных особенностей, включая, те из них, которые позволяют предположить его разработку теми людьми, которые говорят на французском языке.



Название Animal Farm было дано кибергруппе, которая была упомянута канадской организацией Communications Security Establishment (CSE) в серии слайдов презентации, посвященной беглому сотруднику АНБ Эдварду Сноудену в марте 2014 г. В этих слайдах указывается, что к этой группе причастны французские спецслужбы (French intelligence agency). После этого антивирусные компании обнаруживали несколько вредоносных программ, которые были созданы этой кибергруппой.

К этим вредоносным программам относятся:

- Casper, т. н. имплант первого уровня, который был задокументирован ESET.
- Bunny, представляет из себя бэкдор, написанный на языке Lua, он был задокументирован исследователем Marion Marschalek (Cyphort).
- Babar, представляет из себя вредоносное ПО для кибершпионажа, также задокументирован Marion Marschalek.

Связь между этими вредоносными программами и причастность группы Animal Farm была убедительно доказана исследователем компании G DATA Paul Rascagnères. Наше исследование посвящено еще одной вредоносной программе, за которой стоит эта кибергруппа. Она называется Dino.

Общие сведения

Проанализированный нами файл вредоносной программы использовался в 2013 г. в направленных кибератаках против Ирана. Исходный вектор заражения остался неизвестен, однако, мы считаем, что Dino был установлен другой вредоносное программой, так как он содержит в себе процедуры по удалению себя из системы и не содержит аналогичную процедуру установки. Учитывая тот набор команд, которые Dino может получать, мы полагаем, что его основная цель заключается в получении файлов на зараженной системе с последующей их отправкой на удаленный сервер (exfiltration).

Название вредоносной программы было оставлено авторами в ее теле, как и в случае с другой вредоносной программой Casper, о которой мы упоминали выше. Видимо, названием Dino было заимствовано у одного из персонажей мультфильма «Флинстоуны» (The Flintstones). Эта вредоносная программа упоминалась в исследовании антивирусной компании Kaspersky Lab.

В общем, можно сказать, что Dino представляет из себя сложный бэкдор, построенный по модульному принципу. Среди технических особенностей можно упомянуть собственную файловую систему, которая используется для исполнения команд в скрытном стиле, а также специальный комплексный модуль, который исполняется в качестве запланированной задачи (task-scheduling module) и работает аналогично команде *cron* в UNIX. Исполняемый файл содержит множество различных информационных сообщений об ошибках, что позволяет сделать вывод о том, что разработчиками вредоносной программы были люди с очень хорошим знанием французского языка.

Структура вредоносной программы

Вредоносная программа была написана на языке C++ и использует модульную архитектуру. Следующий список модулей вредоносной программы был извлечен из исполняемого файла Dino. Названия модулей были даны самими разработчиками.

Название модуля	Назначение
PSM	Зашифрованная дисковая копия модулей вредоносной программы.
CORE	Хранилище данных конфигурации.
CRONTAB	Планировщик задач.
FMGR	Менеджер передачи файлов.
CMDEXEC	Менеджер исполнения команд.
CMDEXECQ	Очередь хранения команд.
ENVVAR	Хранилище данных переменных окружения.

Dino использует в своей работе специальную структуру данных под названием «DataStore». В частности, все модули вредоносной программы хранят свои данные внутри этой структуры, так что понимание формата и содержания этой структуры является ключом к понимаю работы вредоносного ПО в целом.

Структура DataStore представляет из себя ассоциативный контейнер (map), который хранит ассоциации (соответствия) между ключами строк (string keys) и значениями 8-ми различных типов данных. Реализация этой структуры данных основана на хэш-таблице. Это значит, что для получения значения, которое ассоциировано с ключом, нужно рассчитать хэш этого ключа для нахождения элемента контейнера, из которого будет извлечено значение.

Хэш представляет из себя значение размером один байт, которое вычислено с использованием серии операций XOR на ключе. Каждое значение элемента контейнера представляет из себя голову связного списка, который содержит пары ключ/значение. Ниже представлен фрагмент кода вредоносной программы, который отвечает за извлечение значения, ассоциированного с ключом.

```
// Get the hash of the key to look for
hash = 0x55;
for ( i = arg_key_to_look_for; *i; key_char = *i )
{
  ++i;
  hash ^= key_char;
}
// Look for the key in the linked list starting
// at the index "hash % number of buckets"
for ( current_field = (datastore->array_of_buckets
                       + 4 * (hash % datastore->number_of_buckets));
      current_field;
      current_field = (obj_datastore_field *)current_field->next_field )
{
  // True when the two strings are equals
  if ( !_stricmp((const char *)current_field->key, arg_key_to_look_for) )
    break;
}
```

Структура DataStore также может храниться как простой непрерывный массив в памяти, который начинается со специальной сигнатуры «DxSx». Такой формат хранения используется модулем PSM для хранения содержимого модулей Dino в зашифрованном файле. Когда модулю PSM нужно сохранить эту структуру из памяти в файл на диске, он сохраняет ее именно в таком формате. После перезапуска вредоносной программы, ее код выполняет операцию преобразования этих данных в структуру ассоциативного контейнера. Ключ, который используется для шифрования файла с данными структуры на диске, соответствует строке «PsmIsANiceM0du1eWith0SugarInside».

Как мы уже упоминали выше, изначально данные конфигурации Dino хранятся в виде простого массива (т. н. serialized DataStore object) данных, который хранится в архиве и располагается в конце исполняемого файла вредоносной программы. В процессе своего исполнения эти данные преобразуются в ассоциативный контейнер и сохраняются в памяти внутри модуля CORE. Мы смогли получить список содержимого конфигурационных данных с помощью команды «conf –l CORE», которая будет описана позднее. Ниже представлена эта извлеченная конфигурационная информация.

```
Started:5523F782 QWORD
InitialWaitDone:00000001 DWORD
InteractiveDelay:00000005 DWORD
MaxNothingSaidCount:00000078 DWORD
InstallDate: 5523F782 QWORD
fields:78537844...[REDACTED]...66B3900 BYTES
recID:11173-01-PRS WIDESTR
Version:1.2 WIDESTR
BD_Keys: 4D41474943424F58...[REDACTED]...9EB3506 BYTES
CC_Keys: 4D41474943424F58...[REDACTED]...0000000 BYTES
MaxDelay:00000E10 DWORD
ComServer0:hXXp://www.azhar.bf/...[REDACTED].../postal.php STR
ComServer1:hXXp://www.rsvniima.org/...[REDACTED].../din12/postal.php STR
ComServer2:hXXp://www.azhar.bf/...[REDACTED].../postal.php STR
ComServer3:hXXp://www.rsvniima.org/...[REDACTED].../din12/postal.php STR
ComServer4:hXXp://dneprorudnoe.info//...[REDACTED].../postal.php STR
ComServer5:hXXp://dneprorudnoe.info//...[REDACTED].../postal.php STR
ComServer6:hXXp://dneprorudnoe.info//...[REDACTED].../postal.php STR
NextSendReceive:5CC33097FB72D001 BYTES
CC:000064F7-72E4-3F7D-C817-474D-A9BDBDF7 STR
DaysOfLife:00000000 DWORD
GUID:12FEB4A9EEDEE411B283000C29FD2872 BYTES
InitialDelay:00000000 DWORD
now:5523F78E QWORD
hash:A88E8181CA5CE35AE70C76145DFB820D BYTES
InitialCommands:78537844...[REDACTED]...000000 BYTES
xT0rvwz:DC188352A...[REDACTED]...00000 BYTES
tr4qa589:K/[RAFtIP?ciD?:D STR
jopcft4T:a.ini WIDESTR
```

Предназначение некоторых ключей понятно по их названию, однако, некоторые нуждаются в более подробном объяснении.

- «recID»: киберграппа Animal Farm использует это поле в структуре для идентификации жертвы. В случае рассмотренного нами образца Dino, это поле содержало значение «11173-01-PRS». Другое вредоносное ПО, которое использовалось этой группой – Casper, использовало в качестве значения число 13001, а некоторые образцы Babar использовали значения «12075-01» и «11162-01».
- «ComServer»: эти ключи содержат в качестве значений URL-адреса управляющих C&C-серверов. Все эти адреса уже были недействительными к моменту нашего анализа. В качестве доменов для этих C&C-серверов использовались легитимные веб-сайты, что является обычной практикой для киберграппы Animal Farm.
- «Version»: версия вредоносной программы, в нашем случае, поле было установлено в значение «1.2», что также подтверждается названием директории «din12», ссылка на которую фигурировала в одном из URL-адресов управляющего C&C-сервера. Еще одна директория с названием «d13» была замечена в другом адресе C&C-сервера Animal Farm (см. раздел 3.7 «Calling home» отчета по Babar), что указывает на использование и других версий вредоносного ПО Dino in-the-wild.
- «BD_Keys» и «CC_Keys» содержат криптографические ключи для шифрования трафика сетевого взаимодействия с C&C-сервером. Значения этих ключей начинаются с сигнатуры «MAGICBOX».
- Названия трех последних ключей (см. скриншот выше) хранятся в обфусцированном виде («xT0rvwz», «tr4qa589» и «jopcft4T») и содержат параметры, используемые для работы с файловой системой вредоносной программы.

В следующей таблице указываются команды, которые злоумышленники могут отправить боту. Каждая из команд может иметь один или более аргументов.

Команда	Описание
Sysinfo	Получить информацию о системе.
killBD	Удалить вредоносную программу из системы с использованием собственной файловой системы (см. ниже описание ramFS).
!	Исполнить команду интерпретатора (shell), которая передается в качестве аргумента.
cd	Изменить текущую рабочую директорию.
pwd	Получить путь к текущей рабочей директории вредоносной программы.
dir	Получить список содержимого указанной директории с различной дополнительной информацией.
set	Установить или сбросить переменную окружения, хранящуюся в модуле ENVVAR.
conf	Получить или обновить содержимое указанного модуля.
search	Выполнить поиск файлов по маске имени. Найденные файлы архивируются ботом в специальный архив, который затем планируется на определенное время для отправки на удаленный сервер с использованием модуля FMGR.
archive	Создать архив файлов с указанными путями.
unarchive	Распаковать архив в указанную директорию.
download	Запланировать передачу файла на C&C-сервер с использованием модуля FMGR.
cancel	Удалить запланированную задачу на передачу архива файлов.

Команда	Описание
cancelall	Удалить все запланированные задачи по передаче файлов модулем FMGR.
cronadd	Запланировать выполнение команды на определенное время с использованием модуля CRONTAB (см. описание CRONTAB ниже).
cronlist	Получить список зарегистрированных задач модуля CRONTAB.
crondel	Удалить ранее зарегистрированную задачу модуля CRONTAB.
wakeup	Запланировать «пробуждение» вредоносной программы после определенного времени с использованием CRONTAB модуля.
restart	Команда не реализована.
showip	Получить публичный IP-адрес зараженного компьютера.
cominfos	Получить информацию об используемом вредоносной программой в данный момент C&C-сервере.
comallinfos	Получить информацию обо всех известных вредоносной программе C&C-серверах.
wget	Загрузить файл с текущего C&C-сервера на компьютер.
delayttk	Задержать удаление вредоносной программы, если оно было запланировано.

Одна из вышеперечисленных команд вызывает особый интерес, это команда «search». Она позволяет операторам вредоносной программы осуществлять поиск файлов на скомпрометированном компьютере. Поиск может быть достаточно расширенным и выполняться не только по маске имени, но и по другим характеристикам файла. Например, оператор может запросить поиск файлов с расширением .doc, размер которых больше 10KB и которые подвергались модификации за последние три дня. Мы полагаем, что основное предназначение Dino заключалось именно в краже файлов (exfiltration).

При своем запуске Dino последовательно исполняет команды, которые хранятся в секции «InitialCommands» конфигурационного файла. Проанализированный нами образец содержал следующие команды.

sysinfo

cominfos

!ipconfig /all

!ipconfig /displaydns

!tracert www.google.com

Очевидно, что данные команды используются операторами в качестве осуществления разведки. Их исполнение обеспечивается модулем CMDEXEC, а в памяти команды расположены внутри модуля CMDEXECQ. Результат выполнения этих команд отправляется на C&C-сервер.

RamFS: временная файловая система

Вредоносная программа использует свою (custom) файловую систему под названием ramFS. Она обеспечивает вредоносную программу специальной комплексной структурой хранения данных файлов в памяти, при этом каждый из элементов файловой системы содержит имя файла, используемого обычной дисковой ФС. RamFS также поддерживает набор команд, которые могут размещаться в файлах, а затем выполняться. Следует отметить, что ramFS также присутствует в других вредоносных программах кибергруппы Animal Farm.

Содержимое RamFS изначально хранится в зашифрованном виде в секции файла конфигурации (значение ключа ассоциативного контейнера) под названием «xT0rvwz». Ключ для расшифровки содержимого (RC4) хранится в качестве значения в элементе «tr4qa589». Как только файловая система будет расшифрована, она будет хранится в памяти в качестве связного списка 512-ти байтовых блоков, каждый из которых зашифрован с использованием RC4. При поиске файла в RamFS, вредоносный код будет расшифровывать каждый из этих блоков, затем обрабатывать их, а потом опять зашифровывать. Таким образом работа с файловой системой организуется на должном уровне защищенности.

Ниже указаны некоторые высокоуровневые характеристики этой ФС.

- Название файлов и их содержимое представлено в кодировке Unicode.
- Названия файлов ограничены длиной в 260 символов.
- После расшифровки вредоносный код будет работать с данными файла блоками по 540 байт.
- ФС не ассоциирует с файлом какие-либо метаданные.

Мы не смогли найти какую-либо уже известную файловую систему, структуры данных которой соответствовали бы ramFS, поэтому мы считаем, что эта файловая система является собственной разработкой кибергруппы Animal Farm.

Следующие команды могут быть исполнены вредоносной программой в контексте файловой системы.

Команда	Описание
CD	Сменить текущую директорию на реальной файловой системе.
MD	Команда не реализована.
INSTALL	Установка или удаление вредоносной программы, а также ветки реестра и сервиса.
EXTRACT	Сохранить хранимый в ramFS файл на диске.
DELETE	Удалить сохраненные ранее файлы.
EXEC	Исполнить файл, хранимый в ramFS.
INJECT	Выполнить внедрение хранимого в ramFS файла в контекст запущенного процесса.
SLEEP	Выполнить операцию «Sleep» на заданный промежуток времени.
KILL	Завершить работающий процесс.
AUTODEL	Команда не реализована.

В случае с Dino, ramFS выполняет функцию защищенного хранилища для файла, который содержит инструкции для удаления вредоносной программы из системы. Разработчики Dino называют этот файл деинсталлятором (cleaner) и он выполняется в системе при получении ботом команды «killBD». Ниже на рисунке показан код вредоносной программы, который отвечает за исполнение файла деинсталлятора. Первое что он делает, это получает имя файла из упомянутой выше структуры DataStore («a.ini»), зачем он получает ключ для расшифровки содержимого ramFS. Далее выполняется монтирование файловой системы в памяти для извлечения оттуда и исполнения

файла деинсталлятора. Указанные разработчиками строки с объяснениями дают наглядное представление об осуществляемых вредоносных кодом действиях.

```
// Search for the cleaner file name in Dino configuration
cleaner_file_name = DataStore::SearchForKey(dino_config_datastore, k_cleaner_file_name);
if ( cleaner_file_name && cleaner_file_name->type == WIDESTR )
{
  // Search for the key to decrypt ramFS
  ramfs_crypto_key = DataStore::SearchForKey(dino_config_datastore, k_ramfs_crypto_key);
  if ( ramfs_crypto_key && ramfs_crypto_key->type == STR )
  {
    if ( MountRamFS(...)
    {
      ExecuteCleanerRamFS((int)&var_ramfs_obj);
      DataStore::StoreValue(v14, "results", L"cleaner executed, exiting", a1);
      DataStore::StoreValueFixedSize(arg_datastore, "destroyPSM", 1, 0, 1);
    }
    else
    {
      DataStore::StoreValue(v11, "results", L"Unable to mount cleaner RamFS, exiting", a1);
    }
  }
  else
  {
    DataStore::StoreValue(v10, "results", L"No cleaner Passphrase Found, exiting", a1);
  }
}
else
{
  DataStore::StoreValue(a1, "results", L"No cleaner Script Found, exiting", a1);
}
```

Исполняемый файл деинсталлятора содержит строку «INSTALL -A “wusvcd” –U», которая осуществляет удаление вредоносной программы из системы. Название «wusvcd» использовалось при установке Dino в систему. Следовательно, ramFS используется в качестве защищенного контейнера для файлов, которые будут выполнены вредоносной программой на компьютере пользователя. Таким образом, она предлагает среду исполнения необходимых оператору программ в системе пользователя, которая оставляет очень мало следов.

Планирование задач

Команды «cronadd», «cronlist» и «crondel» используются для добавления, перечисления и удаления запланированных задач модуля CRONTAB. Задачи представляют из себя команды Dino, которые указывались выше. Вредоносная программа использует схожий с командой *cron* синтаксис для планирования задач. В частности, время, на которое запланировано выполнение задачи, указывается строкой следующего формата «минута час день месяц год деньнедели». Кроме этого, эта строка может быть заменена на «@boot» для запуска указанной команды при каждой загрузке системы. Ниже приведен пример вывода команды «cronlist», после того как выполнение команды «wakeup» было запланировано на 7-е апреля 2015 г. в 15:44.

Id	Cron String						Local	Count	Command	Visibility
C1	44	15	07	04	2015	*	-d	-1	wakeup	regular

Как мы можем увидеть, каждый элемент имеет свой идентификатор id, который начинается со значения 0xC0. Назначение поля «Local» остается для нас неясным. Поле «Count» указывает количество раз исполнения команды, значение «-1» означает, что команда должна быть исполнена один раз. Последнее поле «Visibility» указывает на то, будет ли вредоносный код сообщать на свой C&C-сервер об успешности выполнения команды (другое возможное значение «Silent»).

Происхождение Dino

Объем исполняемого кода, который является общим для всех вредоносных программ группы Animal Farm, оставляет мало сомнений в ответе на вопрос о его происхождении. Среди тех особенностей, которые являются общими для этих вредоносных программ, можно привести следующие.

- В самом начале своего исполнения, Dino проверяет имя текущего процесса на совпадение с именами процессов песочниц (sandboxes). На скриншоте ниже показана эта проверка. Схожие проверки («klavme», «myapp», «TESTAPP» and «afyjevmv.exe») присутствуют в образцах Bunny и других образцах вредоносного ПО группы Animal Farm.

```
// Converts the file name to lowercase
_wcslwr_s(Filename, 0x104u);
// Checks the file name against sandbox names
if ( wcsstr(Filename, L"klavme.exe") )
  ExitProcess(0);
if ( wcsstr(Filename, L"myapp.exe") )
  ExitProcess(0);
if ( wcsstr(Filename, L"testapp.exe") )
  ExitProcess(0);
result = (DWORD)wcsstr(Filename, L"afyjevmv.exe");
if ( result )
  ExitProcess(0);
```

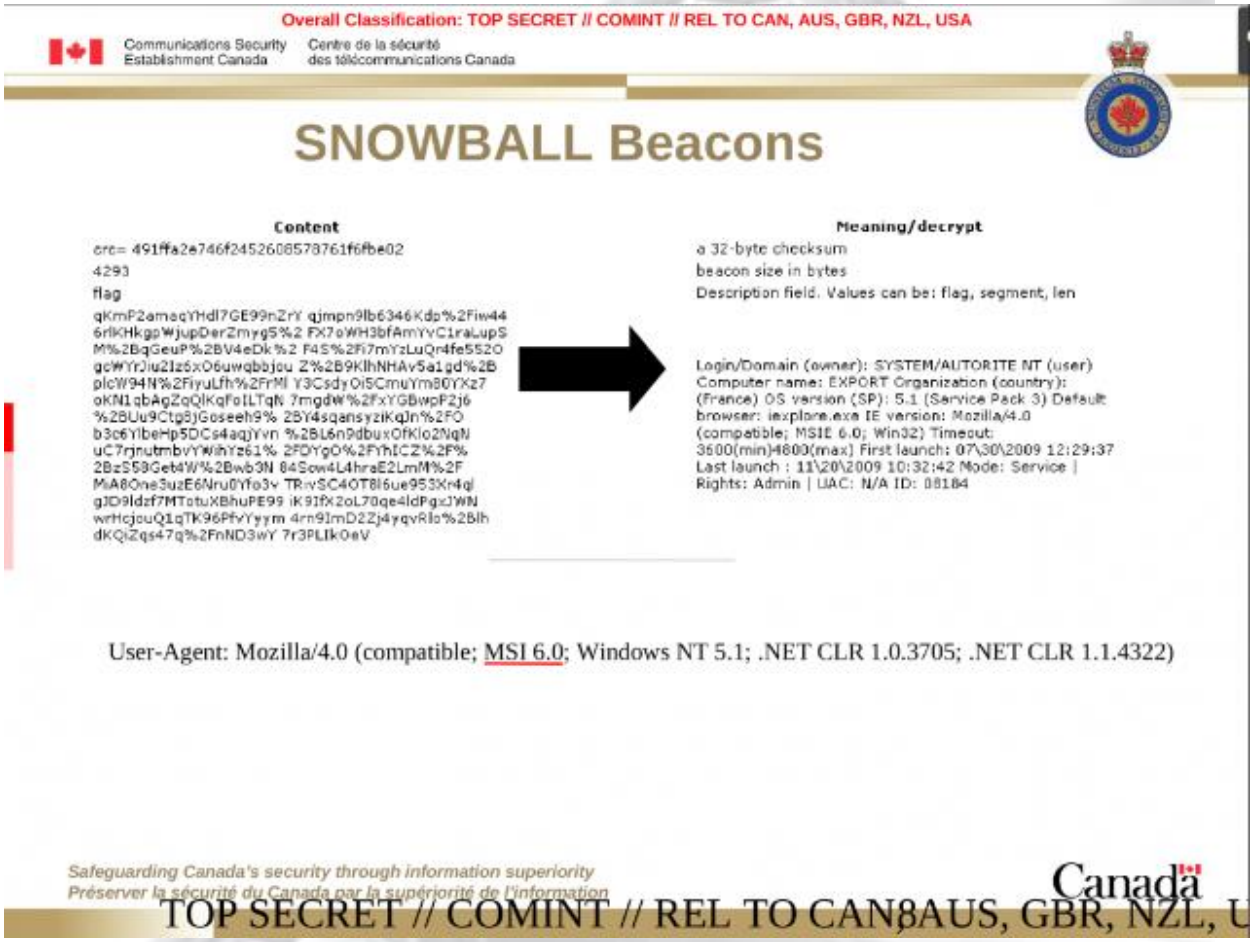
- Для сокрытия вызовов различных API функций, Dino использует метод, который был замечен в использовании другими вредоносными программами Animal Farm: Dino рассчитывает хэш имени функции и использует его для поиска адреса функции в своей таблице. Алгоритм рассчета хэша в Dino схожий с тем, который используется в Casper, он использует комбинацию функции ROL для 7 битов, а также операцию XOR.
- Собственная файловая система Dino, которая называется ramFS, используется и в других вредоносных программах группы Animal Farm. В этих образцах она используется для хранения файлов полезной нагрузки. Например, ниже указана команда ramFS, которая используется некоторыми дропперами NBOT.

```
INSTALL -A "Net3D" -B "Net3d.exe" -D "3D Network Service" -C "3D Network Service" -F
```

- Другим доказательством того, что Dino принадлежит группе Animal Farm является формат вывода команды получения информации о системе. Он очень похож на вывод аналогичной команды обновленной версии компонента «beacon» импланта SNOWBALL, который описывался в упомянутых слайдах CSE.

Dino's sysinfo example output

Login/Domain (owner): Administrator/JOHN (john)
Computer name: JOHN
Organization (country): (United States)
RecId: 11173-01-PRS
MaxDelay: 3600
Version: 1.2
OS version (SP): 5.1 (Service Pack 3)
WOW64: No
Default browser: firefox.exe
IE version: Mozilla/4.0 (compatible; MSIE 7.0; Win32)
First launch: 04/01/2015 – 18:31:14
Time to kill: N/A
Last launch : 04/01/2015 – 19:21:44
Mode: N/A | Rights: Admin | UAC: No
ID: 4635BEF0-D89D-11E4-B283-000C-29FD2872
InstallAv: 0
Inj: Yes



Вредоносная программа обладает как минимум двумя индикаторами того, что она была написана разработчиками с хорошим знанием французского языка.

- Исполняемый файл вредоносной программы содержит ресурс с языковым кодом равным 1036. Основная цель этого ресурса заключается в том, чтобы предоставить разработчикам локализацию необходимых элементов управления (меню, значки, информация о версии) для различных стран на нескольких языках. Следует отметить, что в том случае, когда

разработчик программы не устанавливает это значение кода языка вручную, компилятор устанавливает его в значение кода языка ОС разработчика. Значение 1036 соответствует французскому языку. Мы полагаем, что это значение не является фальшивым, поскольку в некоторых других образцах вредоносного ПО кибергруппы Animal Farm (напр. Casper), код языка был установлен в английский (USA). Похоже, что для тех образцов разработчики Animal Farm просто забыли установить правильное значение языка и исправили ее в случае с Dino. Код 1036 встречался нам не только в образцах Dino, но и в других вредоносных программах группы Animal Farm.

- Исполняемый файл Dino статически скомпонован с библиотекой GnuMP, которая используется для работы с большими числами в криптографических алгоритмах. Этот код в образцах Dino содержит следующие локальные пути. Видно, что в названии директории пути используется французское слово «arithmetique», которое соответствует английскому «arithmetic».

..\..\src\arithmetique\mpn\mul.c

..\..\src\arithmetique\printf\doprnt.c

..\..\src\arithmetique\mpn\tdiv_qr.c

..\..\src\arithmetique\mpn\mul_fft.c

..\..\src\arithmetique\mpn\get_str.c

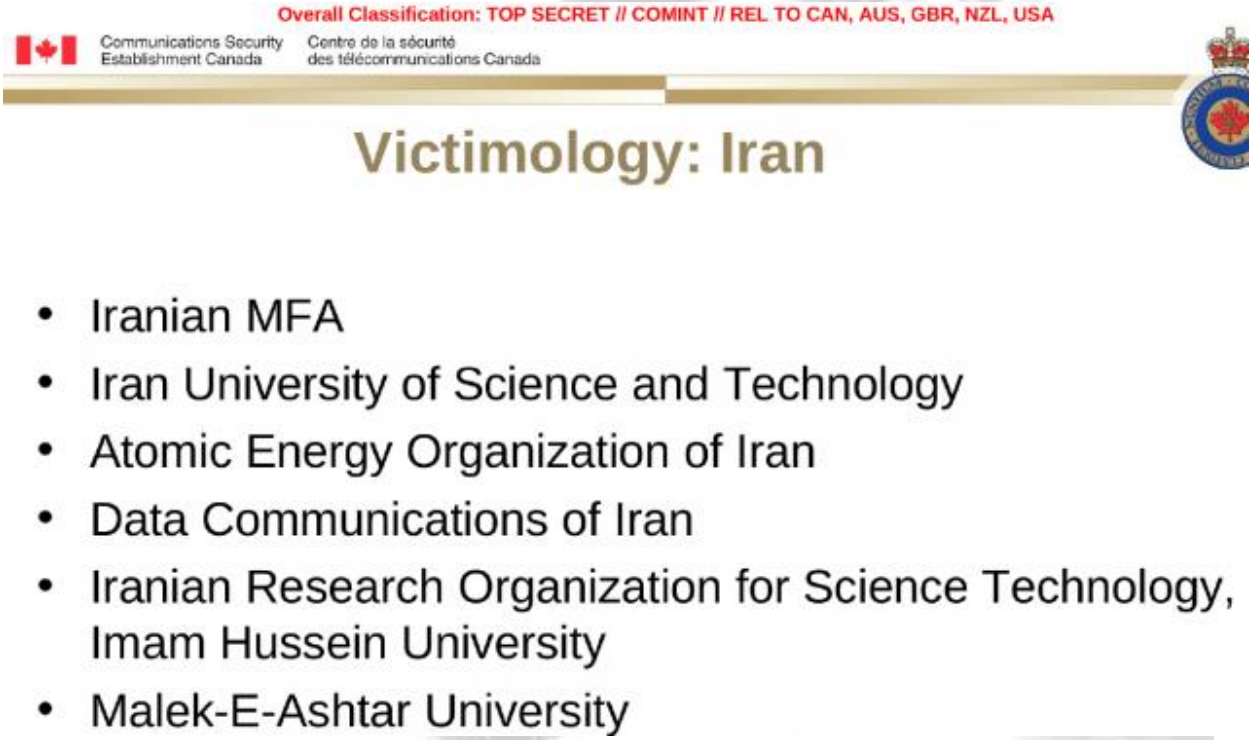
Заключение

Вредоносное ПО Dino демонстрирует хорошую подготовку авторов, которые использовали специальные структуры данных и собственную файловую систему для хранения данных конфигурации и файлов. Как и другое вредоносное ПО группы Animal Farm, Dino является изделием весьма профессиональных и опытных разработчиков. Однако, код Dino демонстрирует плохое знание авторами или просто отсутствие интереса у них к механизмам, препятствующим анализу вредоносной программы, что отличает его от Casper. Тело вредоносной программы содержит множество различных диагностических сообщений, по которым можно предсказать поведение программы.

```
"update ttk with negative of null value is forbidden, consider using
killbd instead"

"update not done, value wasn't already in module and type mispelled or
missed"

"archive %s successfully created, but unable to schedule download.Try
to manually download/erase it."

"Date is invalid ! Date Format is ddmmyyyy"

"decyphering failed on bd"
```

Все эти сообщения существенно облегчают понимание внутренней структуры Dino и выполняемых им действий. Однако, многие из них содержат опечатки.

Что касается жертв Dino, то мы почти ничего не знаем о них. Согласно уже упомянутой презентации CSE, жертвы располагались в Иране. Ниже указан слайд презентации с информацией о жертвах.



Индикаторы компрометации (IoC)

Индикатор	Значение
SHA1 образца	BF551FBDCF5A982705C01094436883A6AD3B75BD
URL-адрес C&C-сервера	hXXp://www.azhar.bf/modules/mod_search/found/cache/postal.php
URL-адрес C&C-сервера	hXXp://www.rsvniima.org/templates/rsv/icons/din12/postal.php
URL-адрес C&C-сервера	hXXp://dneprorudnoe.info/sxd/lang/i18n/charcodes/postal.php
Путь к файлу	C:\Program Files\Common Files\wusvcd\wusvcd.exe
Названия файлов хранилищ	C:\Program Files\Common Files\wusvcd\wusvcd00000000-0000-0000-0000-0000-00000000.{dax,dat,lck}
Расширение загружаемых файлов	.tmp_dwn
Раздел реестра	Software\Microsoft\Windows\Windows\CurrentVersion\Run\wusvcd