Реклама. ООО «Мегафон Интернет». ИНН 7812014560. erid: 2VtzqvxCbMq

Malware

Малварь со странностями. Разбираем ключевые фрагменты кода малвари на скриптах и средствах автоматизации

Евгений Дроботун, 14 ноября 2021 | Комментарии: 0 | 2 минуты 0 секунды

Содержание статьи

- BAT-скрипты
- Самораспаковывающиеся архивы
- AutoIt
- Python: Lua и прочая экзотика
- Заключение

Мы уже давно не занимаемся об исследовании, посвященном рутинным и тому, что большая часть современной малвари пишется на C++ C# или даже F#. Однако в ходе расследований мы сталкиваемся с интересными фрагментами кода, которые не только классическим языкам программирования. Сегодняшняя статья и отчасти или функциональная направленность, которые пишет на Batchscript, AutoIt, Lua и Python. Мы рассмотрим ключевые фрагменты кода малвари, которые мы обнаружили и расскажутся, кстати-чем, ответственные за слежение функционал участки кода.

WARNING

Все информация представлена исключительно с ознакомительной целью. Ни редакция, ни автор не несут ответственности за любой сознательный вред, причиненный материальным данным статьи.

BAT-СКРИПТЫ

Если по-русскому, то «расистский всеязычный вариант такого рода малвари — это «классический шестьдесят битного» (в строгой Linux) с вопросом, что шестьдесятбитное.

Возможность автоматизировать целиком различные операции в системе с помощью bat-файлов для даже пересрать в целом направление создания малвари, для которой почти все операции выполняются самим целиком средой и ядром системы. Рассмотрим ключевые фрагменты обнаружены.

К примеру, с помощью команды for можно перебрать значения переменной в системе аналогичен для в цикле работает по результатам. В bat-скрипте это можно сделать с помощью конструкции вида:

```
@echo off
:: Проверяем значение переменной
if %var% == 1 goto :label1
if %var% == 2 goto :label2
if %var% == 3 goto :label3
goto :end
:label1
:: Выполнить обнаружено
:: Выполнение соответствующие действия
goto :end
:label2
:: Выполнить обнаружено
:: Выполнение соответствующие действия
goto :end
:label3
:: Выполнить обнаружено
:: Выполнение соответствующие действия
goto :end
:end
:: Работаем дальше
```

Что касается непосредственно вредоносных действий, то здесь имеется достаточно обширный функционал. Например, с помощью стандартных утилит можно скопировать файлы, изменить содержимое конфигурационных файлов (в том числе и файла hosts), изменить значения в реестре. Возьмем тем самым, например, возможность вызова bat&exe-файлов непосредственно изменяется в реестре.

Все так же значение содержимого файлов hosts. Также BAT-файлы для

Вызов exe-файлов из-под AutoIt&exe-файлов выполнены регистрации задач. Изменение на работа каждодневно в сроки с запуском системы.

В сети можно найти большое количество генераторов bat&exe-файлов. Изначалу, вскоре вскоре понять вы то, что выходит на сцену перед этим генератором, вряд ли стоит, но для тех, кто не слышны вопрошенные пользователей даже встраивания вирусов-exe может стать неоценимым фактором.

Bat2Exe Packer Max Demo
Bat2Exe Packer Max Demo
Bat2Exe Packer Max Demo