EXPONENTA FOR WINDOWS

EXPONENTA FOR WINDOWS Manual Page

NAME

exponenta - модульный админ пак для Microsoft Windows

DESCRIPTION

Exponenta содержит в себе набор скриптов и утилит для управления и первоначальной настройки компьютера под управлением операционной системы Microsoft Windows. Скрипты управляют реестром Windows, открывают удалённый доступ к компьютеру и т.д. Смотри описание утилит и скриптов ниже.

AUTHOR

Exponenta была написана Юрием Денисовым

RESOURCES

GitHub: http://github.com/yudenisov/Exponenta

Main web site: http://yudenisov.ru

COPYING

Exponenta Admin pack

Год,дата выпуска: 2019

Copyright: © New Internet Technology Inc., 2016-2019

Лицензия: BSD (Open Source)

Разрядность: 32 bit

Поддерживаемые платформы: Microsoft Windows XP SP3, Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows 10, Windows 2003 Server SP1, Windows 2008 Server R2, Windows 2012 Server R2, Windows 2016 Server, Windows 2019 Server,

Админ пак «Экспонента» (Exponenta) представляет собой модульное средство, выполняющее следующие функции:

1. Управление реестром Windows;

2. Предоставление удалённого доступа к компьютеру;
3. «Жёсткая блокировка» антивирусов и автоматического обновления Windows;
4. Активация и дезактивация защиты от программы mimikatz;
5. Добавление в компьютер «универсальной учётной записи» для удалённого доступа;
6. Получение внешнего IP адреса компьютера (при помощи запроса к сторонним сервисам);
7. Проверка системной информации о компьютере;
8. И многое другое, неочевидное для пользователя.

Функциональность админ пака расширяется плагинами, которые также являются самостоятельными программными продуктами, переупакованными автором админ-пака.

Админ-пак устанавливается в каталог %PUB1%\Util (по умолчанию C:\pub1\Util). Инсталлятор представляет собой Inno Setup EXE файл, устанавливающий в папку по умолчанию основные скрипты, а также устанавливающий переменные окружения. Скрипты затем запускаются из комендной строки. Из соображений безопасности запрещается автозапуск этих скриптов после установки.

Внимание! Админ пак может быть использован в злонамеренных целях, например, для написания вредонсной программы-стайлера. Именно поэтому многие «параноидальные антивирусы», типа Avast Free Antivirus, опознают дистрибутив с данными скриптами как malware (вредоносное программное обеспечение), в то время как другие антивирусы (ESET NOD32, Kaspersky Internet Security) выдают предупреждающее сообщение о возможной его потенциальной опасности. Автор заявляет, что в дистрибутиве нет и не может быть по определению вирусов, а злонамеренность в применении скриптов лежит на пользователе и администраторе, их запускающем. Сами по себе скрипты также не содержат вредоносного кода.

Категория: Админ-паки | ***Добавил:*** yudenis | **Теги:** Админ пак, Exponenta, Windows 7, Windows Server, Windows 10, admin-pack, new internet technologies, Windows XP SP3

Состав продукта

В данный админ-пак входят следующие скрипты, файлы и утилиты:

adAdminDomain.cmd
файл создания учётной записи MSSQLSR с паролем и наделение её правами локального администратора компьютера

adAdminLocal.cmd
файл создания учётной записи MSSQLSR с паролем и наделение её правами локального администратора компьютера

before.exe

Программа приостанавливает выполнение командного файла до отметки времени startTime, и продолжает выполнение до отметки времени EndTime
Программа полезна, если Вы по каким-то причинам не хотите использовать планировщик заданий.
Usage: BEFORE.EXE starttime [endtime] [nowait]

check_reg_item.bat

check_reg_item checks the item «item» at node «node» for value or default value
Usage check_reg_item.bat «node» «item»
Проверяет пункт «item» на присутствие значения или значения по умочанию в звене «node» реестра Windows

check_reg_node.bat

check_reg_node checks the node «node» for default value
Usage check_reg_item.bat «node»
Проверяет на существование звена «node» в реестре Windows (со значением по умолчанию)

check_uname_present.bat

check_uname_present.bat is a file for checking some user login to be present in Windows
Usage: check_uname_present.bat «username»
where «username» is windows logon to be tested
Проверяет, что некоторый логин пользователя присутствует в Windows

choc_pack.install.cmd

Пакетный файл для инсталляции программ через менеджер пакетов Chocolatey

chock.install.cmd

Инсталлятор менеджера пакетов Chocolatey

curdaterename.bat

(Бонус) программа для вставки в конец имени файла текущей даты и времени

curdatetimerename.bat

(Бонус) программа для вставки в конец имени файла текущей даты и времени

datetimemsec.exe

Данная команда делает отметку текущего времени, с разделителем или без
Usage: datetimemsec.exe [/delims]
Вывод «YYYY[delims]MM[delims]hh[delims]mm[delims]ss[delims]Msc»
для использования в команде FOR /F, и использования «случайных» строк

deAdminDomain.cmd

файл удаления учётной записи MSSQLSR с паролем и наделение её правами локального администратора компьютера

deAdminLocal.cmd

файл удаления учётной записи MSSQLSR с паролем и наделение её правами локального администратора компьютера

dis-lsaprotect.cmd

скрипт дезактивации защиты LSA на компьютерах с Microsoft Windows 7 - 10

dis-somemimikatz-features.cmd

скрипт для дезактивации некоторых особенностей операционных систем, необходимых для успешного запуска программы Mimikatz. Программа бесполезна для Windows 10

dis-wdigest.cmd

скрипт для дезактивации WDigest протокола на компьютерах с Windows 7 -10

edlinw32.exe

файл - строковый редактор для правки файлов на удалённом компьютере в CLI WinRS или Telnet сессии.
Это один из немногих редакторов, работающих в этих сессиях. Остальные требуют запуска полноценного терминала.

en-lsaprotect.cmd

скрипт активации защиты LSA на компьютерах с операционной системой Microsoft Windows 7 - 10

en-somemimikatz-features.cmd

скрипт, включающий некоторые возможности системы, необходимые для запуска программы mimikatz. Скрипт бесполезен в Windows 10

en-wdigest.cmd

скрипт, включающий WDigest протокол авторизации

example_check_uname_admin.bat

пример программы, проверяющей, имеет ли текущая запись права локального администратора.

getip_1.cmd

программа для получения внешнего ip адреса системы с помощью сайта ipinfo и программы curl. Программа сохраняет найденный IP АДРЕС В c:\pub1\Util\MyIp.txt

getsysteminfocheck.cmd

(Бонус) Проверка системной информации о компьютере средствами операционной системы Windows. Необходимо для продолжения взлома. Требует установки дополнительного программного обеспечения (см. текст скрипта).

inkeys.exe

Функция возвращает Errorlevel = число ASCII Code нажатой клавиши или 0
Usage: INKEYS.EXE [[string1] prompt_string]
;(c) mak_soft@mail.ru
any params - suppress this help message. Return only Errorlevel Number and ERRORLEVEL
if string1 is nubmer - wait key number of seconds
ERRORLEVEL=0 -no key pressed
ERRORLEVEL=ASCII code of key

любой параметр выводит это сообщение. Выводит только число Errorlevel
Если строка 1 число, то программа ожидает нажатия на клавишу это число секунд.
ERRORLEVEL = 0 - клавиша не нажата
ERRORLEVEL = ASCII коду нажатой клавиши
Команда незаменима при построении интерактивных диалоговых оболочек в Commnd Shell

minifilters-interface-restore.cmd

Восстановление доступа к minifilters, в том числе должны заработать антивирусы.
Внимание! После восстановления доступа необходимо сделать Manual Restart Services!

minifilters-interface-stop.cmd

принудительная остановка minifilters Windows, в том числе всех антивирусов. Возможны баги!

PartOfDomain.bat

скрипт WMI, который проверяет, является ли данный компьютер частью домена, и выдающий информацию о домене.

reg_add_envvar.bat

командный файл добавления системной переменной окружения вместе со значением
Usage: reg_add_envvar.bat «variable name» «value»
где «variable name» имя системной переменной, «value» её значение

reg_addtopath.bat

командный файл для добавления пути к системной переменной Path
Usage: reg_addtopath.bat «Path name»
где «Path name» путь, добавляемый в переменную Path

reg_del_envvar.bat

reg_del_envvar.bat is a script which delete the environment variable from the shell
Скрипт, удаляющий системную переменную окружения из оболочки
Usage: reg_del_envvar.bat «variable name»
где «variable name» имя системной переменной

reg_del_node.bat

reg_del_node.bat is a script to delete of a Windows Registry Node only if reserve copy is created
Скрипт, который удаляет раздел «node» из реестра Windows только если создана резервная копия «file name with extension»
Usage: reg_del_node.bat «node» «file name with extension»

reg_export_reserve.bat

reg_export_reserve.bat is a script to make of a reserved copy of the Windows Registry Node
If Old reserve copy is present, it is assigned name backupp1-5 with warning and then

return warning or general error
Скрипт, создающий резервную копию раздела реестра Windows.
Usage: reg_export_reserve.bat «node» «file name with extension»
где «node» имя раздела реестра, «file name with extension» резервная копия ветви реестра. Расширение нужно указывать явно (обычно оно reg).

reg_import_file.bat

reg_import_file.bat is a script to add into the Windows Registry a file «file» with check of his presistens
Скрипт, импортирующий файл в реестр Windows с проверкой файла на существование
Usage: reg_import_file.bat «file name with extension»
где «file name with extension» - файл с резервной копией куста реестра (обычно имеет расширение .reg). Расширение нужно указывать явно.

reset_route.cmd

скрипт для очистки кэша DNS и таблицы маршрутов операционной системы. Скрипт используется, когда компьютер по каким-то причинам не может получить доступ к определённым узлам в Интернете, и это не проблемы провайдера.

Restart_Explorer.bat

скрипт перезапускает системные процессы Explorer.exe и dwm.exe. Применяется, когда окна и элементы управления ведут себя «неподобающим образом» или зависают. Запускается от имени администратора компьютера.

Secure-001.cmd

скрипт удаляет правила брандмауэра, заданные программой UnSecure-001.cmd

Secure-002.cmd

скрипт настраивает программы удалённого доступа telnet, rdp и winrm

Secure-003.cmd

скрипт удаляет шару со всех локальных дисков и диска C:

Secure-004.cmd

скрипт запрещает анонимный доступ к шаре и нулевую сессию для SMB протокола

ShareAllDiscs.cmd

скрипт расшаривает все диски на компьютере (может не работать)

telnet_start.cmd

скрипт запускает службу КруМ Telnet SSH Server v1.19a

telnet_stop.cmd

скрипт останавливает службу КруМ Telnet SSH Server v1.19a

timemer.exe

Программа измеряет время между двумя событиями (метками)
TimeMer (c) 2003 by Michael Korotkin

Usage: timemer.exe string start|stop|view
где string - временная метка (строка символов)
return ERRORLEVEL: 0-254 number of hours, 255 - error
ERRORLEVEL: 0-254 число часов,
ERRORLEVEL=255 - ошибка

tredo_restart.cmd

скрипт перезапускает интерфейс tredo. Вместо номера интерфейса 13 поставьте номер своего tredo интерфейса

uninstall-mainexponenta.cmd

удаление системных переменных окружения Main Exponenta Files
Используется для деактивации или удаления стайлера. После запуска этого файла стайлер работать не будет!

uninstall-stealerexponenta.cmd

удаление системных переменных окружения Main Exponenta Files
Используется для деактивации или удаления стайлера. После запуска этого файла стайлер работать не будет!

UNSECURE_ALL.cmd

контейнер для всех скриптов UnSecure. Обращаться с осторожностью!

Unsecure-001.cmd

This script Adds Firewall Rules, Which allow next task

1. Allowed all ftp connections by ftp.exe program
2. Allowed all telnet connections on ports 23 and 972
3. Allowed all winrm connections on port 5985
4. Allowed all ssh connections on port 22
5. Allowed all rdp connections on port 3389
6. Allowed all RAdmin connections on port 4899
7. Allowed all SMB Shared Connections on port 445
8. Allowed All RPC Connections on Ports 135, 137, 139
9. Allowed Remote Meterpreter Connections on Port 4444
10. Adjust System Services for Autostart

Скрипт добавляет правила брандмауэра, разрешающие следующие задачи:

1. Разрешает все соединения программе FTP.EXE

2. Разрешает соединения telnet по портам 23 и 972
3. Разрешает WinRM соединения на порт 5985
4. Разрешает SSH соединения на порт 22
5. Разрешает RDP соединения на порт 3389
6. Разрешает RAdmin соединения на порт 4899
7. Разрешает SMB шару на порту 445
8. Разрешает SMB и RPC соединения на портах 135, 137, 139
9. Разрешает удалённые Meterpreter соединения на порт 4444
10. Настраивает автостарт системных сервисов.

Unsecure-002.cmd
скрипт настраивает программы удалённого доступа telnet, rdp и winrm

Unsecure-003.cmd
скрипт расшаривает локальный диск C:

UnSecure-004.cmd
скрипт делает возможным запуск планировщика задач Windows, разрешает нулевую сессию SMB протокола и анонимный доступ к шаре.

unsecure-winrm-client.cmd
скрипт включает некоторые небезопасные настройки WinRM клиента. Используйте, если Вам не удалось установить WinRM соединение штатными средствами

unsecure-winrm-service.cmd
скрипт включает некоторые небезопасные настройки WinRM сервера. Используйте, если Вам не удалось установить WinRM соединение штатными средствами

update-chocolatey.cmd
скрытое обновление всех программ, установленных менеджером пакетов chocolatey

winlogon-SpecialAccounts.reg

регистрация аккаунта MSSQLSR как специального
В специальный аккаунт Microsoft Windows нельзя зайти локально (только удалённо), и он не показывается в списке аккаунтов для входа в Windows 7-10

wupdate-interface-restore.cmd

Восстановление доступа к Windows Update Schedule.
Внимание! После восстановления доступа необходимо сделать Manual Restart Computer!

wupdate-interface-stop.cmd

принудительная остановка Windows Update Schedule. Возможны баги!
Обновления indows переводятся в ручной режим.

descript.ion

описание каталога (этот файл в кодировке ANSI CP-1251)

Все скрипты и утилиты являются консольными, запускаются на выполнение из консоли (терминала) Microsoft Windows, с указанием префикса пути «%PUB1%\Util\».

WHAT NEWS

Version 2.0.1.2_beta

- (Add) Some Mimikatz Features Enable/Disable
- (Add) Unsecure WinRM Options
- (Add) Some New Auxiliary commands

Version 2.0.0.0_beta

- (Modify) Some changes at Stealer Installation files and their documentation
- (Fix) Telnet Server Start/stop at AdminT Package
- (Modify) Geek Uninstaller & AeroAdmin New Versions
- (Remove) All Threads From Main Packet

Version 2.0.0.0_alpha

- (Modify) Installer of Admin Pack. Now Plugins Installer is not Part of Exponenta Admin Pack Installer
- Clean OLd Data and Documentation
- Change Directory Structure in Distributive
- Create New Project for NIT Environment

Version 1.8.5.0_alpha

- (Add) Clean old files before update Expoinenta for Windows

- (Add) Update Modules for Windows XP/Windows 2003
- (Add) Modules For Simple Chocolatey Installation
- (Fix) Change Compression Method for Avast Free Antivirus
- (Add) Copyright information for Legal Purples
- (Add) Now Some Modules is Installed at Windows XP SP3
- (Add) Distribution at SVN Server
- (Add) Meterpreter Backdoor Service in Stealer (not Tested)
- (Add) Threads Installer in Stealer (not Tested)
- Rewrite SendFile for Stealer

Version 1.8.4.0_alpha

- (Add) New Scripts at Exponenta For Linux
- (Delete) Some Unwanted Programs by Antivirus
- Some Little Improvements

Version 1.8.3.2_alpha

- (Fix) Time to Start Stealer
- (Fix) DonГўв‚¬в„ўt sent the system information of the styler
- (Fix) Remove Viruses From AdminT
- Some Little Improvements in Modules

Version 1.8.3.1_alpha

- (Fix) Stealer does not receive the commands from server
- (Fix) System Info Module doesnГўв‚¬в„ўt work
- Change The documentation
- Add references to create host web server for stealer management
- Some Little Improvements in Modules
- Add Resources (Icons) to Admin Pack

Version 1.8.3_alpha

- (Fix) Files is not downloaded by curl program
- (Fix) External IP address is not recognized
- (Fix) Minifilters interface stop Error

- Add Windows 10 Feature to stop Windows Update Scheduling
- Add PowerRun program in addition to devxexec program

Version 1.8.2_alpha

- Create working packet of Exponenta for Linux Admin Pack

Version 1.8.1_alpha

- Some little changes in Windows Scripts
- Add Unsecure Rules for Firewall to Make Available Some Server Daemons

Version 1.8.0 Alpha

- Add main modules for Exponenta Linux Admin Pack Install and work
- Add a documentation for Linux Modules
- Correct modules of Exponenta Windows Stealer Main File (clean distributive)

Version 1.7.0 beta

- Change the documentation (was made more friendly and law correct)
- Began to add Exponenta for Linux

Last updated 2019-08-11 08:30:08 +04