Trick 2:

You maybe w

<filename>:<

If we create a . The first trick abused ctory.

However, it’s .txt”, we write in realit equal

because $DA ternet (or receive it via xecute it). For example, the /r switch with t

Side note: Th
C:\Windows\

This behavio
programmer
the set ACL.

For example,
application a
user uploads
applicationFo

Another inter
the native Wi

This on it’s o
see the refer
allows to upl
could lead to
However, an

Trick 3:

Every folder
directory. On
the dots.

he
r because of

r, the
ach). If the
red inside

e files using

his blog;
on IIS and
itized, this
ith it).

arent
sers with

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

The screensh
::$INDEX_AL

The “...” folde
example (mk

Using the se

he “....”

Incident?

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

On older vers However,
on Windows

Incident?

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • **Privacy Statement**

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

Anonymous evaluation for troubleshooting and further development

no yes

Matomo

Matomo.org

SHOW DETAILS

The ADS on ‘ NUL doesn’t have any affe

Please note t ever, it will show the AD

Incident?

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

The red mark Therefore, to hide from

There exists ill automaticall

However, we ke “xyz. .” will automati

Here is the p

Incident?

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

The created

Side note 1:

Side note 2:

We can also

Incident?

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

Then it’s not

Moreover, th tant).

If we can ad

Incident?

Side note 1: ... however, files in it can't be op... e stuck in an endless loop... ne the folder to a name ju... doesn't work). To op...

Filesyst...

I did a quick ... . The most noteworthy f... commands:

```
copy eica...
copy eica...
echo 123...
cd "foo.
copy ..\e...
copy ..\e...
```

After that I re... er, but not the eicar viru... ucts found them (becau... and has therefore no ... the "eicar.com" f... that only files which a... n the file guard setting... file). I also conducted a ... isk image). The "..." folde... "va... the content "... spa... end) is intepr... od... everything is ...

We use Cookies

We use cookies to offer you a perfect visit experience. These include cookies that are necessary for the operation of the site and for the control of our commercial corporate goals, as well as those that are only used for anonymous statistical purposes, for convenience settings or to display personalized content. Decide for yourself which categories you want to allow. Please note that based on your settings, not all functions of the site may be available.

Legal Notice • Privacy Statement

Technically required (0 Service)

no yes

Analysis / statistics (1 Service)

no yes

Anonymous evaluation for troubleshooting and further development

Matomo

no yes

Matomo.org SHOW DETAILS

We created 3

- “file” with t
- “file. .” whi
- “filex x” wh

We now nee remove the
“. .” from the

The above co e
However, we e function
which makes eakpoint. At
the breakpoi his address
is the pointer to our file name.

Incident?

The filename
– that’s why
overwrite the
the filename
ed. Let’s

After that jus

Correct, “file.
ties of “file”
(taskmgr) wi

But what is w
before
NtCreateUse

Moreover, yo

Similiar trick ass the restriction. C

^"%Localappd

to start calc.

This blog pos ere already documented the following refe am. More information c

REFERE

https://msdn

https://tyrani

https://tyrani

https://googl

https://googl

https://googl

http://insert-

https://bogne

https://sec-c

Edit history:

2018-06-13: S n IIS5.1 and a similiar tric

https://sorou

https://sorou

2018-06-14: D

https://githul

https://www.

2018-06-14: C

https://gist.g

https://oddva

https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/