



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

Matomo.org

[SHOW DETAILS](#)

no yes

Home / Blog

Pentester's

12.06.2018

In this blog post, we will explore the use of cookies on the SEC Consult website.

process

powershell editor

Security-headers

ShellExploit

file

MacBook

type

LPC Port

esktop

irectory

irectory

le

le

le

le

le

ay



CAREER ABOUT US CONTACT FN ▾



Lab Blog

Type:

Applies to:

Advanced

Permissions

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

Matomo.org

[SHOW DETAILS](#)

no yes

e folders in

Moreover, it's
it.

This ACL can
and Windows

C:\WIN
C:\Windows
Access i
C:\Wind
The syst
C:\Wind
Volume
Volume
Directo
30.01.20
30.01.20
30.01.20

As shown ab
escalation if

Side note: Th

Contact



Incident?



CAREER ABOUT US CONTACT FN ▾

X

Lab Blog

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](#)

Trick 2:

You maybe w

<filename><

If we create a
trick abused

However, it's
write in realit
because \$DA
receive it via
For example,
switch with t



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

26.02.2018
26.02.2018
26.02.2018

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](#)

As you can see, we can type if we really want to an ADS account.

the \$DATA can be copied

Side note: This process involves

executing WMIC

You maybe a explorer.exe to add an ADS to (number). Then

play them; / – we can be a

For example, that files in C create files a

ns assume users can

Let's say the start at the end For C:\Windows this folder bu

Incident? his


[CAREER](#) [ABOUT US](#) [CONTACT](#)

EN ▾

X [Lab](#) [Blog](#)

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](#)

he
r because of

e files using

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



Incident?

Trick 3:

Every folder in a directory. On the dots.



CAREER ABOUT US CONTACT FN ▾

X
Lab Blog

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](#)

no yes

he "...."



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

clicking
theMoreover, it's
such a folder
explorer char

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

Matomo.org

[SHOW DETAILS](#)

no yes

er and where

ang/search

forever, witho

Please note:



Incident?



CAREER ABOUT US CONTACT FN ▾

Lab Blog

tiVirus
est\''

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.

Trick 4:

[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](#)

ges) a

s the file as
irectory

the file to the

eck time of

ACTION trick

r, in the case
1 point to

nt to



Incident?



CAREER ABOUT US CONTACT

Lab Blog

Lab Blog

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

I'm not sure I
whitelisting

Trick 5:

As already di
dump the str



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 versions of Windows

However,





CAREER ABOUT US CONTACT FN ▾

X

Lab Blog

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

Matomo.org

[SHOW DETAILS](#)

no yes

The ADS on
have any affe

NUL doesn't

Please note i
show the AD

ever, it will



Incident?



CAREER ABOUT US CONTACT FN ▾

X

Lab Blog

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](#)

Therefore,

ill

like "xyz. ."



Incident?



CAREER ABOUT US CONTACT FN ▾

X
Lab Blog

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?



CAREER ABOUT US CONTACT FN ▾

X

Lab

Blog

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

tant).

Moreover, the

If we can add



Incident?


[CAREER](#) [ABOUT US](#) [CONTACT](#) [EN](#)

[Lab](#) [Blog](#)

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](#)

Side note 1:
it can't be op
endless loop
to a name ju
work). To op

ever, files in
e stuck in an
ne the folder
doesn't

Filesystem

I did a quick
noteworthy f

. The most
commands:

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

After that I re
the eicar virus
them (because
therefore no
"eicar.com" f
files which a
guard setting
conducted a
The "... folde
the content "
end) is integr
everything is

er, but not
ucts found
and has
the
that only
n the file
file). I also
isk image).
va
spa
od



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

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 need

remove the

". ." from the

The above co
However, we
which makes
the breakpoi
is the pointer to our file name.



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

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 filename
ed. Let's

ties of "file"

before



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

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](#)

no yes

^ at any
ast symbol
last

a length of
r. However,
ent variable

it should not



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

Moreover, yo

Similiar trick

restriction. C

^%"Localapp

to start calc.

This blog pos

documented

following ref

information o

REFERE

[\[\\[\\\[\\\\[\\\\\[\\\\\\[\\\\\\\[\\\\\\\\[Edit history:\\\\\\\\]\\\\\\\\(https://sec-c</div>
<div data-bbox=\\\\\\\\)\\\\\\\]\\\\\\\(https://bogn</div>
<div data-bbox=\\\\\\\)\\\\\\]\\\\\\(http://insert-</div>
<div data-bbox=\\\\\\)\\\\\]\\\\\(https://googl</div>
<div data-bbox=\\\\\)\\\\]\\\\(https://googl</div>
<div data-bbox=\\\\)\\\]\\\(https://googl</div>
<div data-bbox=\\\)\\]\\(https://tyrani</div>
<div data-bbox=\\)\]\(https://tyrani</div>
<div data-bbox=\)](https://msdn</div>
<div data-bbox=)

2018-06-13: S

a similiar tri

[\[2018-06-14: D\]\(https://sorou</div>
<div data-bbox=\)](https://sorou</div>
<div data-bbox=)[\[2018-06-14: O\]\(https://www.</div>
<div data-bbox=\)](https://github</div>
<div data-bbox=)[\[<https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/>\]\(https://oddva</div>
<div data-bbox=\)](https://gist.g</div>
<div data-bbox=)

Incident?



CAREER ABOUT US CONTACT FN ▾

Lab Blog en.

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](#)



Incident?