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

Windows

By looking at

Therefore, it

```
[…]
detection
    selec
        -
        -
    - 'msiexec.exe'
```

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**

- Isolate, wh
- Block the i
  sources lik
- If support i

Conclus

By analyzing ware in the early stages

As stated by like Emotet or IcedID and prevent the execution of

[1] Initial acce in.
[2] Sysmon (Sy , network connections

Repositories:

Sigma: https

Velociraptor: docs/blob/d8

Yara: https://

Are you

SEC Consult

Incident?

company specializes in information security management, NIS security audits, penetration testing, ISO 27001 certification support, Cyber Defence and secure software certification. SEC Consult is part of Eviden.

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**