



## 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

[ACCEPT SELECTED](#)

[REJECT ALL](#)

[ACCEPT ALL](#)



CAREER ABOUT US CONTACT FN ▾



Lab Blog

BumbleBee t

Bumble

BumbleBee i  
subsequently

- Verifie
- to VM

[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](#)

Malware

The BumbleBee

File

Mi

Sh

Sh

BumbleB

cmd.exe /c cas

item32)\

exe &amp;&amp; start /

twork.dll,

The ISO file a

This PC



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](#)

no  yes



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 )

Anonymous evaluation for troubleshooting and further development

no  yes

#### Matomo

Matomo.org

[SHOW DETAILS](#)

no  yes

Defense

BumbleBee a  
Stream (ADS)

Velocirap

The Velocira  
Logs with Ev

The following

Masque

The technique  
executable in

Velocirap

Velociraptor  
actors.

SELECT \*



Incident?

The following



## 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  
selected

- '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 )

Anonymous evaluation for troubleshooting and further development

no yes

### Matomo

Matomo.org

[SHOW DETAILS](#)

no yes



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

control

The Yara rule  
servers.

## 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

Windows

Since at time  
drive, as shown

external

To detect thi

```
title: Su  
ruletype:  
author: A  
date: 202  
descripti  
reference  
id: aaff3  
status: e  
tags:  
- att  
- att  
logsource  
category  
product: Win  
detection:
```



Incident?



CAREER ABOUT US CONTACT FN ▾



Lab Blog

condi  
level: me

## 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



Incident?

Velocrap

To automatically extract the C2 server addresses from the malware, SEC Defence created further Velociraptor artifacts that firstly detects BumbleBee processes and secondly extracts the IP addresses which have port 443 associated.



CAREER ABOUT US CONTACT FN ▾



Lab Blog

descripti

## 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](#)

]  
- name:  
default  
r

sources:  
- preco  
SEL  
query  
T  
L  
-



Incident?

AND NOT Pid in me.Pid



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

The following

Network

Another met  
network secu



Incident?

In this specif

- ET CNC Fe
- ET CNC Fe
- ET CNC Fe
- ET CNC Fe
- ET CNC Feodo Tracker Reported CnC Server group 25: 95[.]168[.]191[.]248



# 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

Metamorpha

[SHOW DETAILS](#)

## <sup>2</sup> Sysmon (Sy) connections

Sigma: <https://sigma.readthedocs.io>

Yara: <https://>

# Are you

SEC Consult



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](#)



Incident?