APT

okiem reversera

$ **who**ami

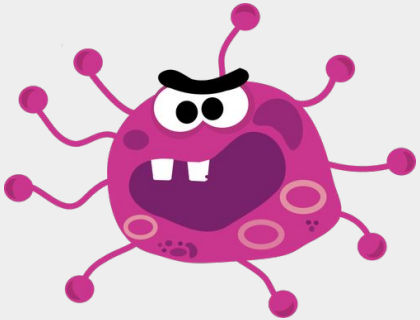
Jarosław Jedynak
msm@tailcall.net

$ **who**ami

Jarosław Jedynak
msm@tailcall.net
(tytułowy reverser)

Analiza
złośliwego
oprogramowania

Symantec

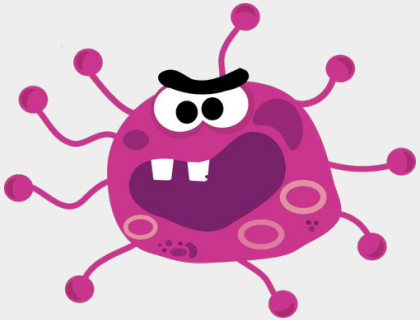


$ **who**ami

Jarosław Jedynak
msm@tailcall.net
(tytułowy reverser)

Analiza
złośliwego
oprogramowania

Symantec

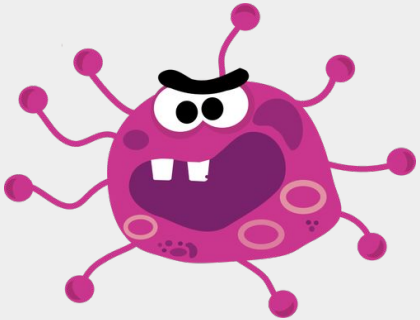


$ **who**ami

Jarosław Jedynak
msm@tailcall.net
(tytułowy reverser)

Analiza
złośliwego
oprogramowania

Symantec



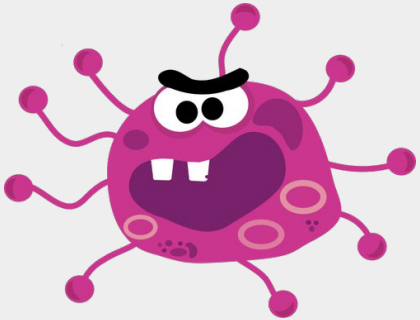
CTF @ p4.team
w “wolnym” czasie

$ **who**ami

Jarosław Jedynak
msm@tailcall.net
(tytułowy reverser)

Analiza
złośliwego
oprogramowania

Symantec



CTF @ p4.team
w “wolnym” czasie

Historycznie
inne zajęcia

CERT.PL

MOBILTEK
BRILLIANT MINDS

część 1

słowem wstępu

Agenda:

- Co to w ogóle jest APT? Kto za nimi stoi?
- Jak wygląda na co dzień praca przy analizie?
- Studium przypadku i dużo dygresji

Agenda:

APT, to brzmi dumnie. W praktyce, jest z tym różnie. Autor, po latach spędzonych na analizie ""konsumenckiego"" złośliwego oprogramowania, odkrywa świat targetowanych ataków, które z jednej czasami budzą podziw poziomem zaawansowania, a z drugiej strony wbrew pozorom często sa rutynowe i wcale nie tak odkrywcze.

Podczas tej prezentacji porozmawiamy o tym jak działają ataki APT (z naciskiem położonym na Targetowane, nie na Zaawansowane), jak się na nie poluje, jaka w tym rola reverse-engineera, oraz czy da się przed nimi bronić. Nie będzie to wbrew pozorom ciężka technicznie prezentacja - ograniczymy slajdy z kodem asemblera, zamiast tego prześledzimy ""łańcuchy zabójstw"" (kill chains) oraz schematy ataków. Wszystko zostanie zaprezentowane na przykładach realnych ataków (ale tylko tych, które już są publicznie znane :)).

Agenda:

APT, to brzmi dumnie. W praktyce, jest z tym różnie. Autor, po latach spędzonych na analizie ""konsumenckiego"" złośliwego oprogramowania, odkrywa świat targetowanych ataków, które z jednej czasami budzą podziw poziomem zaawansowania, a z drugiej strony wbrew pozorom często sa rutynowe i wcale nie tak odkrywcze.

Podczas tej prezentacji porozmawiamy o tym jak działają ataki APT (z naciskiem położonym na Targetowane, nie na Zaawansowane), jak się na nie poluje, jaka w tym rola reverse-engineera, oraz czy da się przed nimi bronić. Nie będzie to wbrew pozorom ciężka technicznie prezentacja - ograniczymy slajdy z kodem asemblera, zamiast tego prześledzimy ""łańcuchy zabójstw"" (kill chains) oraz schematy ataków. Wszystko zostanie zaprezentowane na Przykładzie realnego ataku (ale tylko tych, które już są publicznie znane :)).

Agenda:

Dygresja

APT, to brzmi dumnie. W praktyce, jest z tym różnie. Autor, po latach spędzonych na analizie ""konsumenckiego"" złośliwego oprogramowania, odkrywa świat targetowanych ataków, które z jednej czasami budzą podziw poziomem zaawansowania, a z drugiej strony wbrew pozorom często sa rutynowe i wcale nie tak odkrywcze.

Podczas tej prezentacji porozmawiamy o tym jak działają ataki APT (z naciskiem położonym na Targetowane, nie na Zaawansowane), jak się na nie poluje, jaka w tym rola reverse-engineera, oraz czy da się przed nimi bronić. Nie będzie to wbrew pozorom ciężka technicznie prezentacja - ograniczymy slajdy z kodem asemblera, zamiast tego prześledzimy ""łańcuchy zabójstw"" (kill chains) oraz schematy ataków. Wszystko zostanie zaprezentowane na przykładach realnych ataków (ale tylko tych, które już są publicznie znane :)).

Gdzie jest "Targetowane" w APT? 🤔

WTF is APT?

Computing and software [edit]

- APT (programming language) (Automatically Programmed Tool), a high-level computer prog
- APT (software), Debian's high-level package management system, also used by other Linux
- Almost Plain Text, or Doxia, a wiki-like syntax used mainly by Apache Maven
- Annotation processing tool, a utility for executing annotation processors in the Java progran
- Advanced persistent threat, a set of stealthy and continuous computer hacking processes
- Applied Predictive Technologies, a statistical business analysis software company
- Advanced Programming Techniques Ltd., creators of the Command CICS software product

WTF is APT?

Computing and software [edit]

- APT (programming language) (Automatically Programmed Tool), a high-level computer prog
- APT (software), Debian's high-level package management system, also used by other Linux
- Almost Plain Text, or Doxia, a wiki-like syntax used mainly by Apache Maven
- Annotation processing tool, a utility for executing annotation processors in the Java progran
- Advanced persistent threat, a set of stealthy and continuous computer hacking processes
- Applied Predictive Technologies, a statistical business analysis software company
- Advanced Programming Techniques Ltd., creators of the Command CICS software product

WTF is APT?

Advanced

Persistent

Threat

WTF is APT?

Advanced?

Lapsus$? Hacktivism?
Ransomware groups?

Persistent

Threat

WTF is APT?

Advanced?

Lapsus$, Hacktivism,
Ransomware groups

Persistent?

Attacks as short as days,
Ransomware groups

Threat

WTF is APT?

Advanced?

Lapsus$, Hacktivism,
Ransomware groups

Persistent?

Attacks as short as days,
Ransomware groups

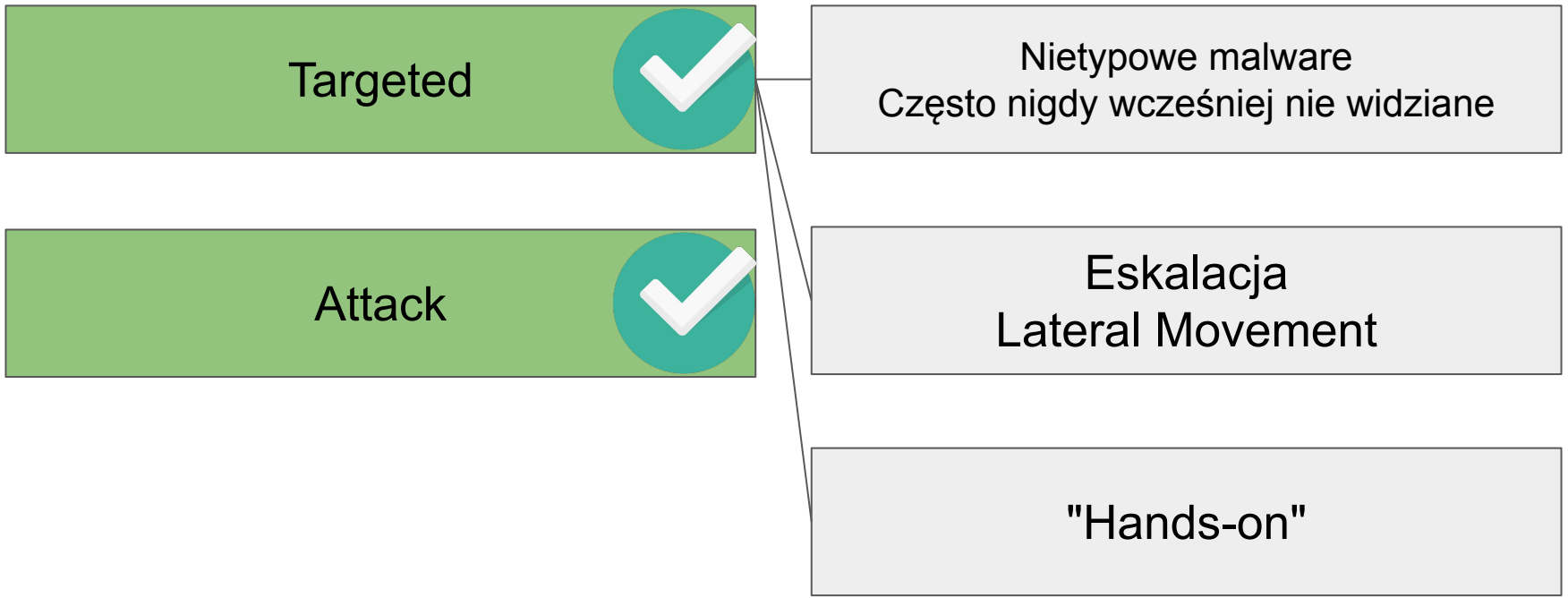
Threat

Targeted Attack?

Targeted 

Attack 

Targeted Attack?



Attack Groups

Nie jest łatwo za nimi nadążyć.

Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium**

Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

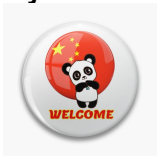
- **MenuPass** (FireEye)

Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

- **MenuPass** (FireEye)
- 🥇 **Stone Panda** (Crowdstrike)

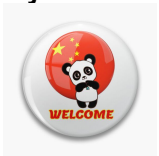


Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

- **MenuPass** (FireEye)
- 🥇 **Stone Panda** (Crowdstrike)
- 🥈 **APT 10** (Mandiant)

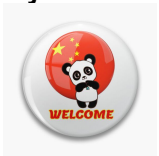


Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

- **MenuPass** (FireEye)
- 🥇 **Stone Panda** (Crowdstrike)
- 🥈 **APT 10** (Mandiant)
- https://en.wikipedia.org/wiki/Red_Apoll



Red Apollo

From Wikipedia, the free encyclopedia

This article is about the threat actor. For the butterfly, see Parnassius epaphus. For the element, see Potassium.

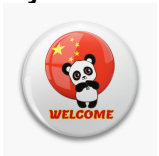
Red Apollo (also known as **APT 10** (by Mandiant), **MenuPass** (by Fireeye), **Stone Panda** (by Crowdstrike), and **POTASSIUM** (by Microsoft))
A 2018 indictment by the United States Department of Justice claimed that the group is linked to the Tianjin State Security Bureau of Chinese

Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

- **MenuPass** (FireEye)
- 🥇 **Stone Panda** (Crowdstrike)
- 🥈 **APT 10** (Mandiant)
- https://en.wikipedia.org/wiki/Red_Apoll



Red Apollo

From Wikipedia, the free encyclopedia

This article is about the threat actor. For the butterfly, see Parnassius epaphus. For the element, see Potassium.

Red Apollo (also known as **APT 10** (by Mandiant), **MenuPass** (by Fireeye), **Stone Panda** (by Crowdstrike), and **POTASSIUM** (by Microsoft))
A 2018 indictment by the United States Department of Justice claimed that the group is linked to the Tianjin State Security Bureau of Chinese

- 🥉 **Cicada** (Symantec)

Attack Groups

Nie jest łatwo za nimi nadążyć.

Grupa APT **Potassium** znana również jako:

- **MenuPass** (FireEye)
- 🥇 **Stone Panda** (Crowdstrike)
- 🥈 **APT 10** (Mandiant)
- https://en.wikipedia.org/wiki/Red_Apoll

Red Apollo

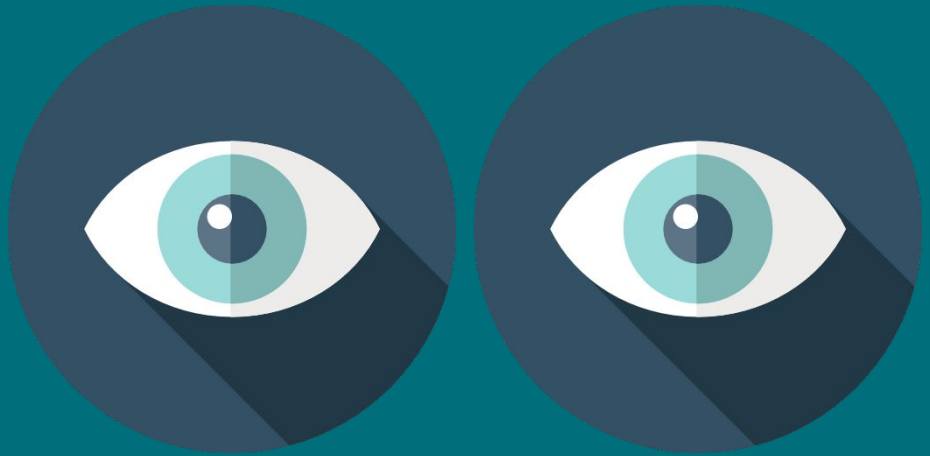
From Wikipedia, the free encyclopedia

This article is about the threat actor. For the butterfly, see Parnassius epaphus. For the element, see Potassium.

Red Apollo (also known as **APT 10** (by Mandiant), **MenuPass** (by Fireeye), **Stone Panda** (by Crowdstrike), and **POTASSIUM** (by Microsoft))
A 2018 indictment by the United States Department of Justice claimed that the group is linked to the Tianjin State Security Bureau of Chinese

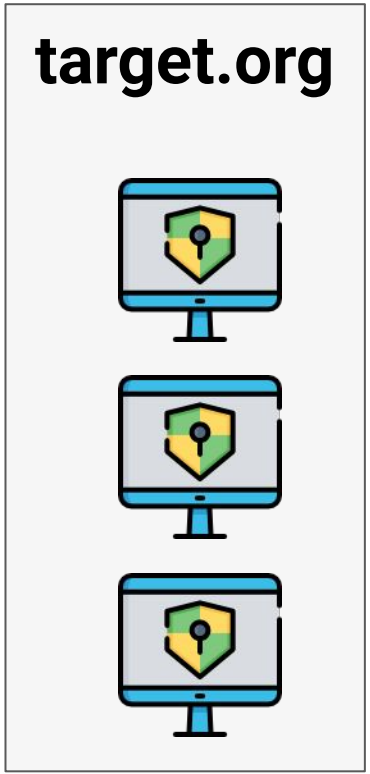
- 🥉 **Cicada** (Symantec)
- ...i więcej

część 2



organizacją pracy

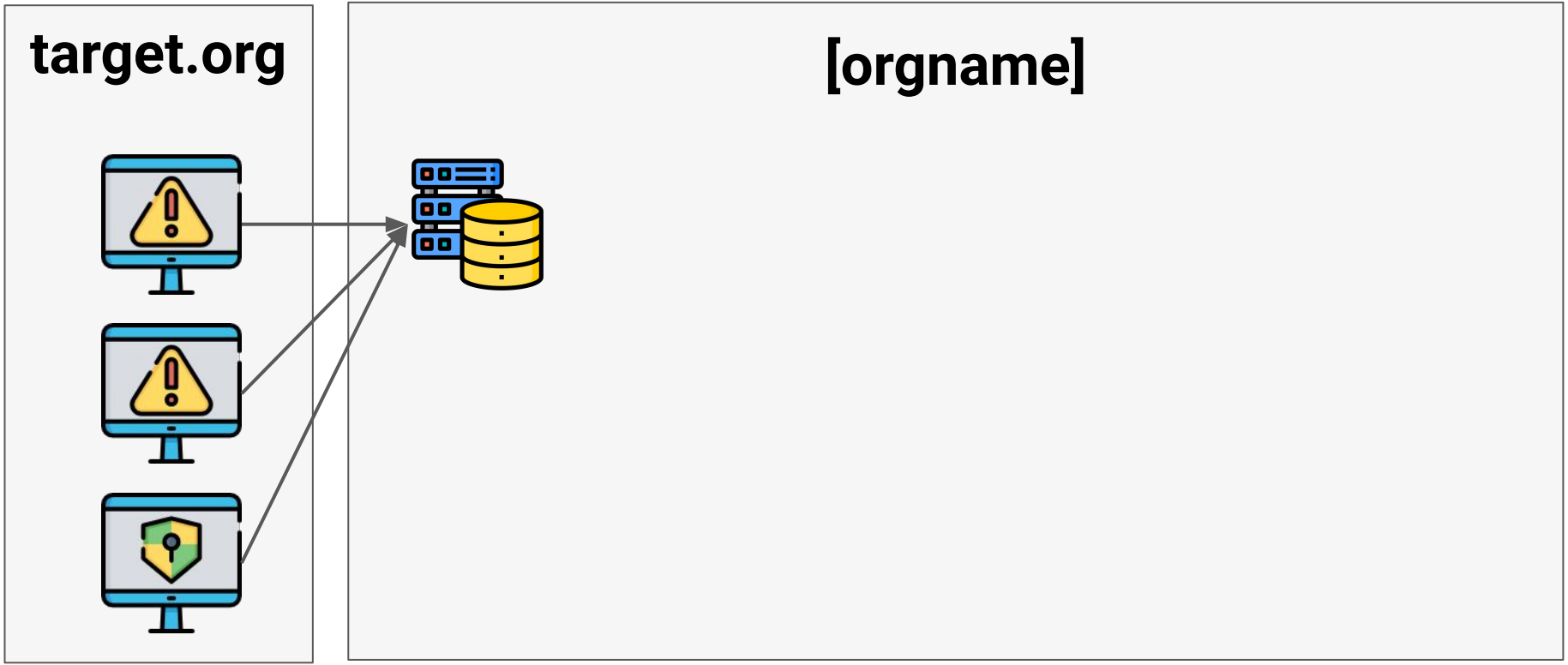
Organizacja pracy



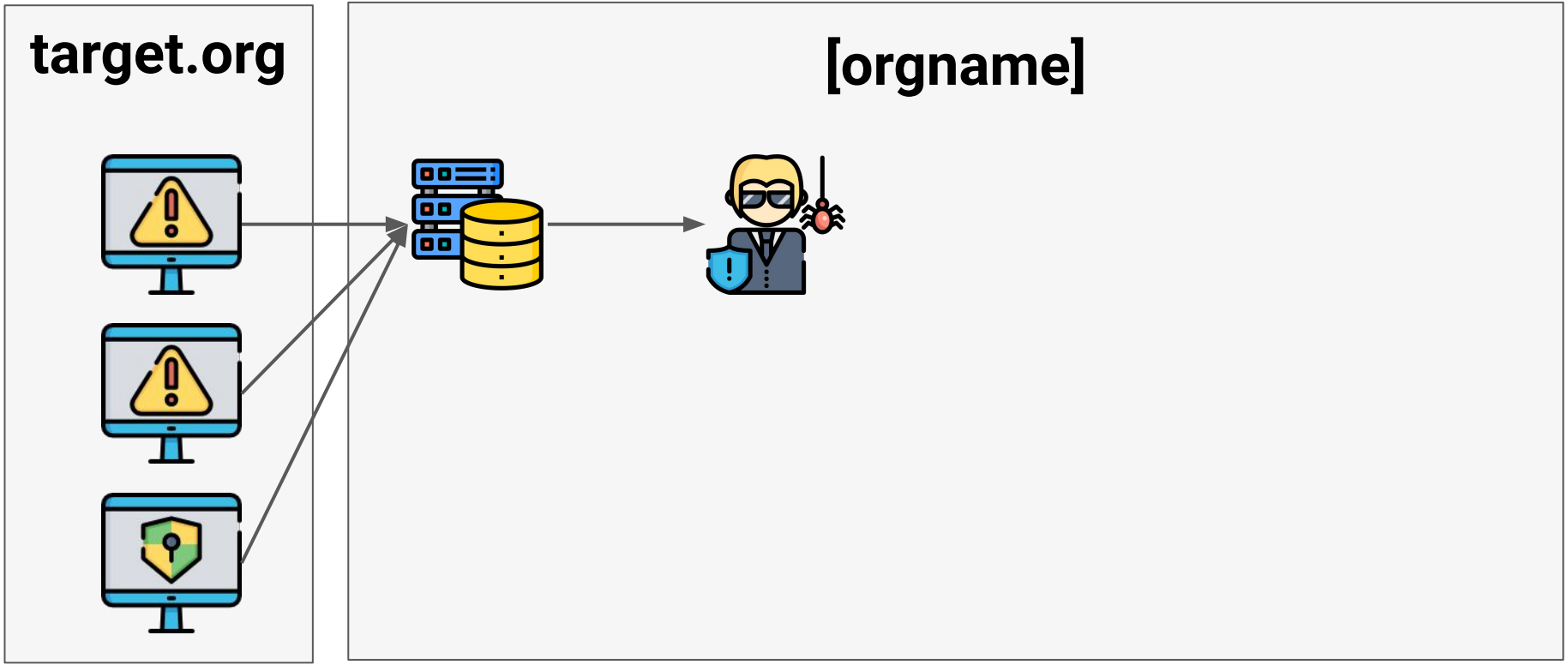
Organizacja pracy

target.org

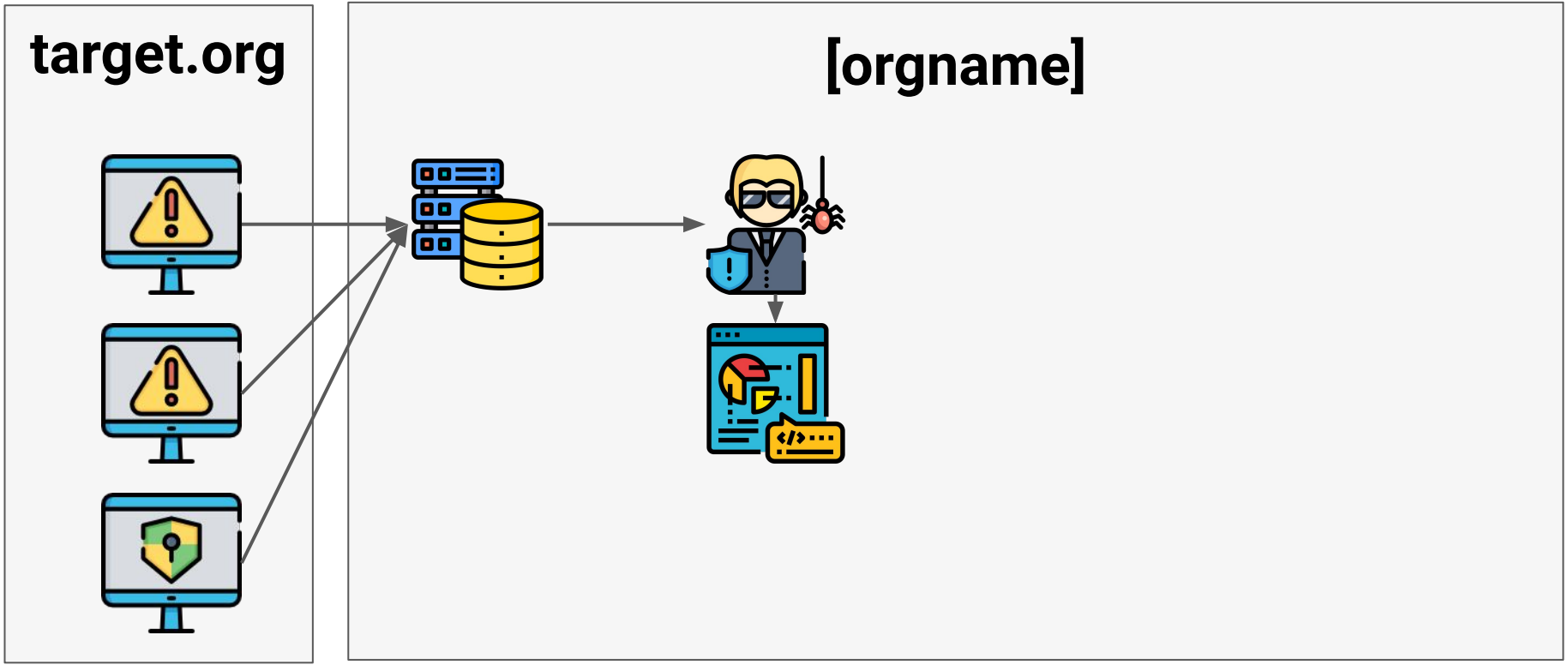
Organizacja pracy



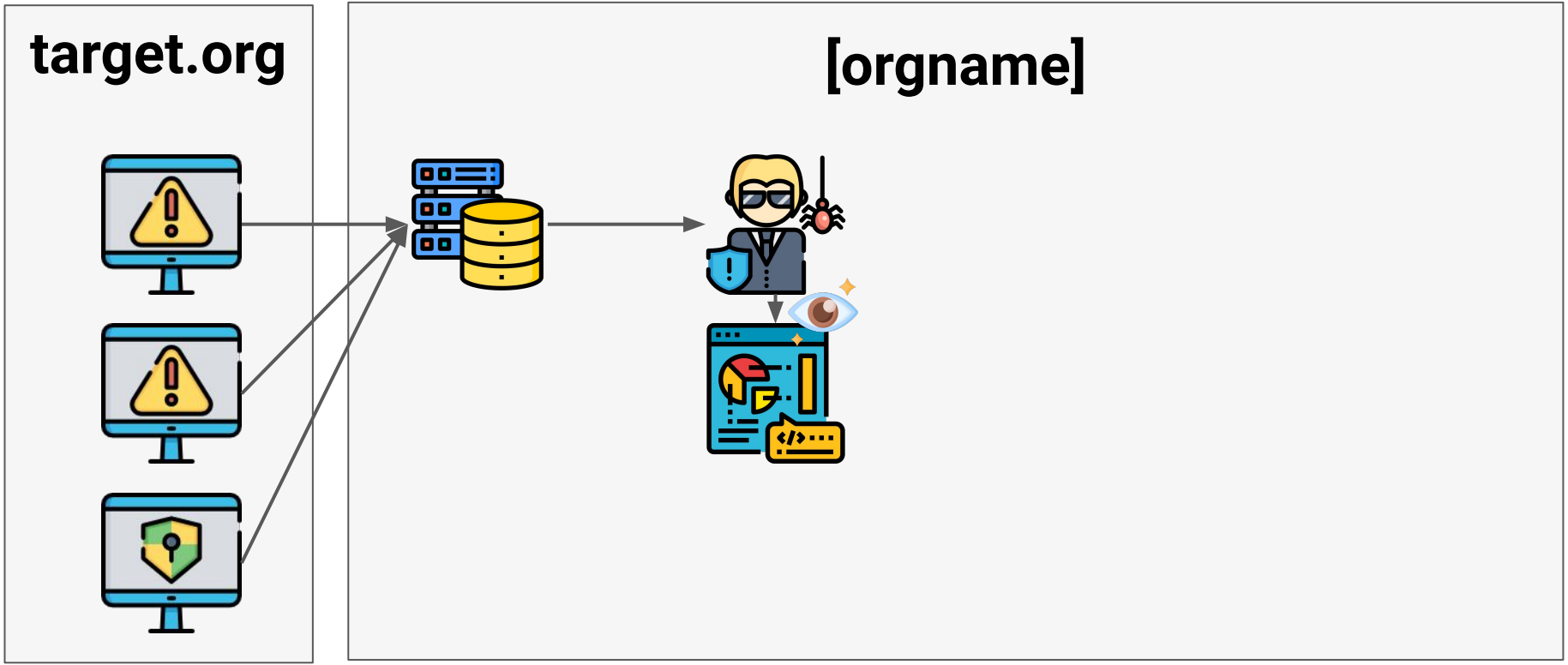
Organizacja pracy



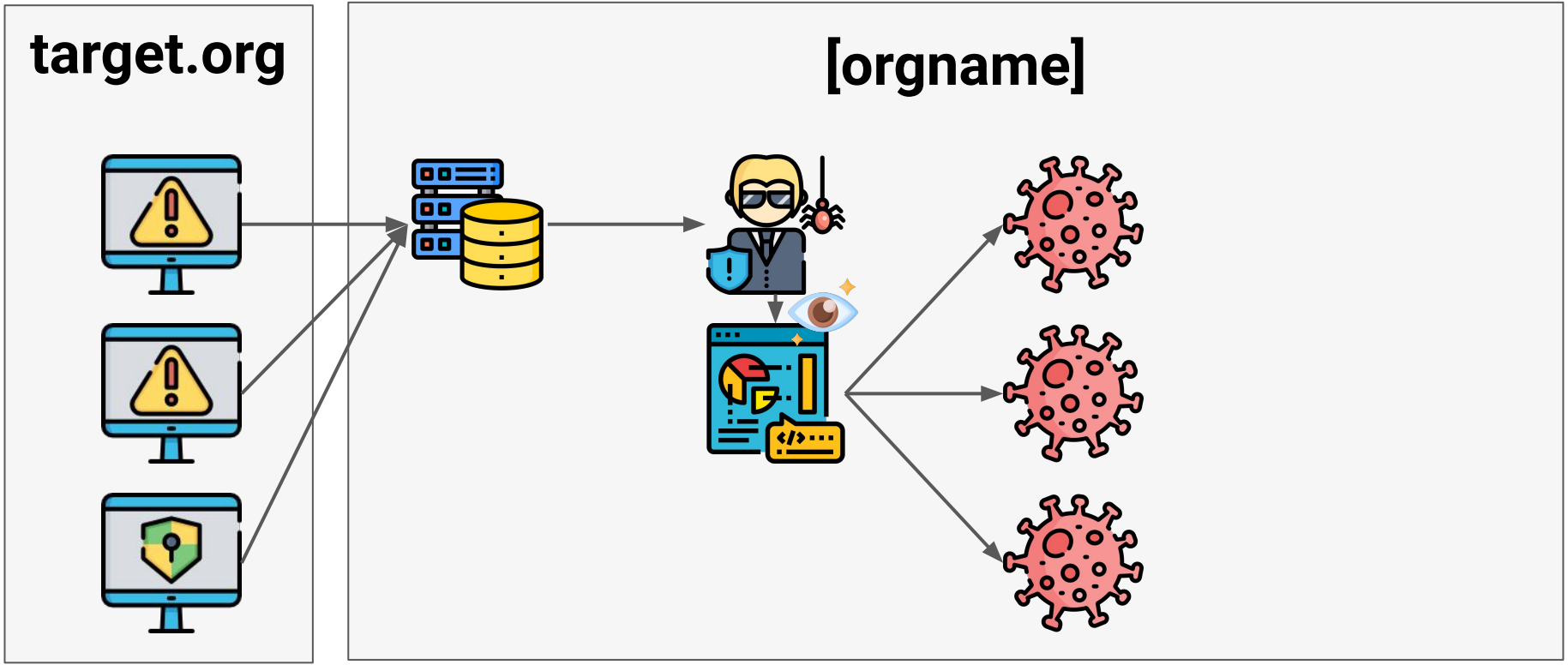
Organizacja pracy



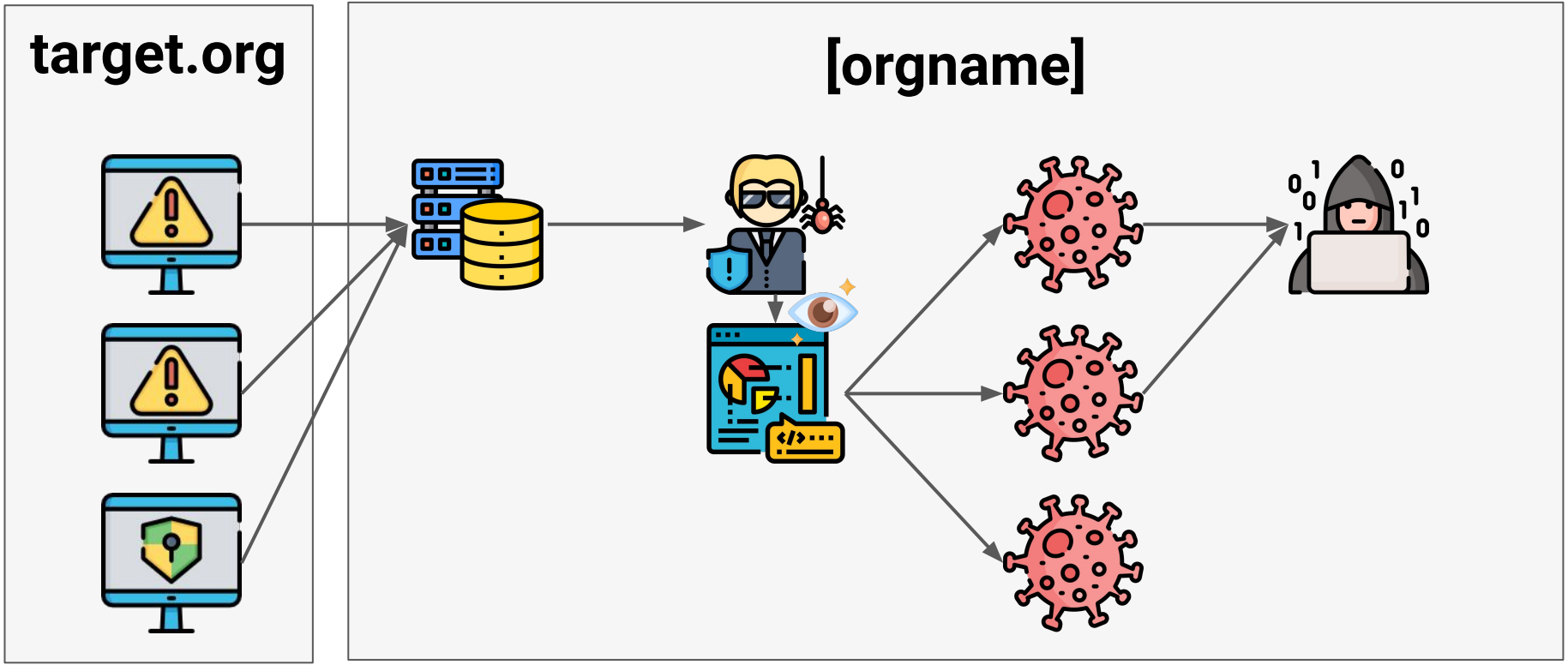
Organizacja pracy



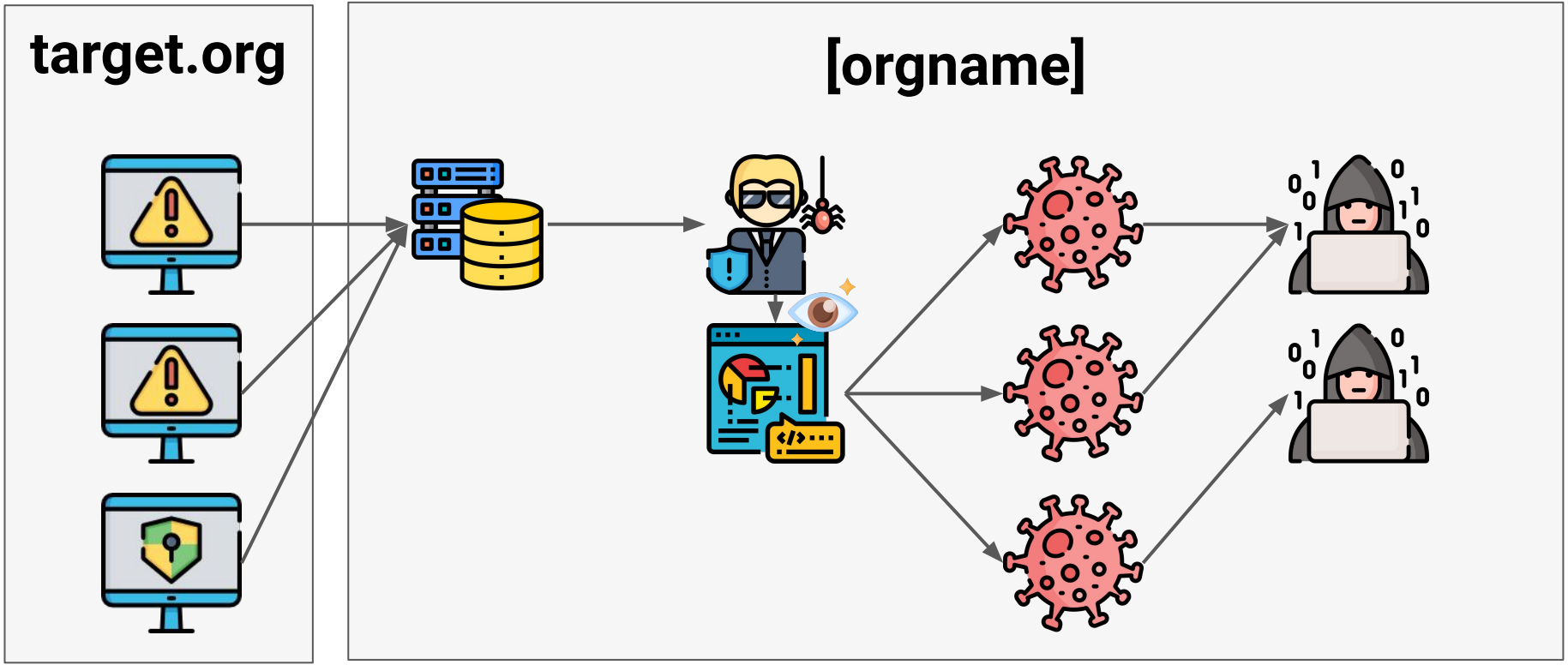
Organizacja pracy



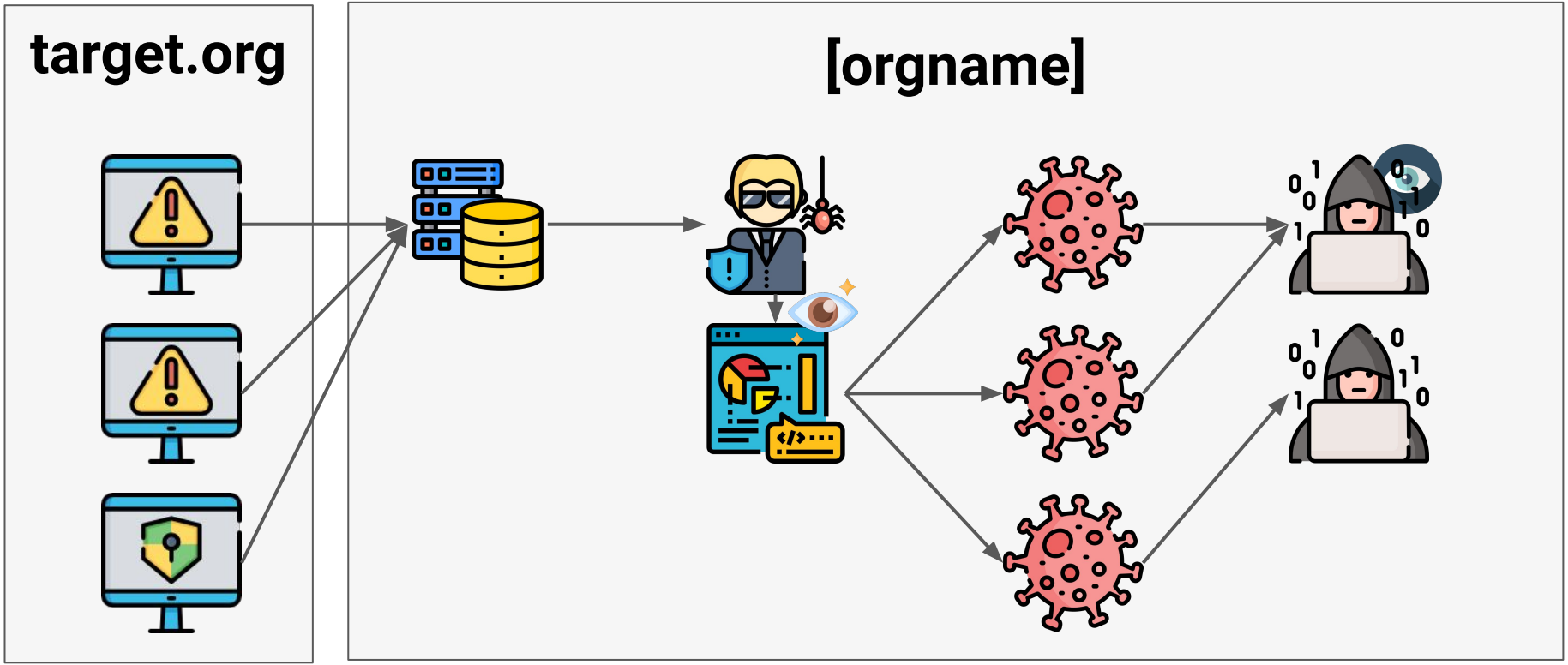
Organizacja pracy



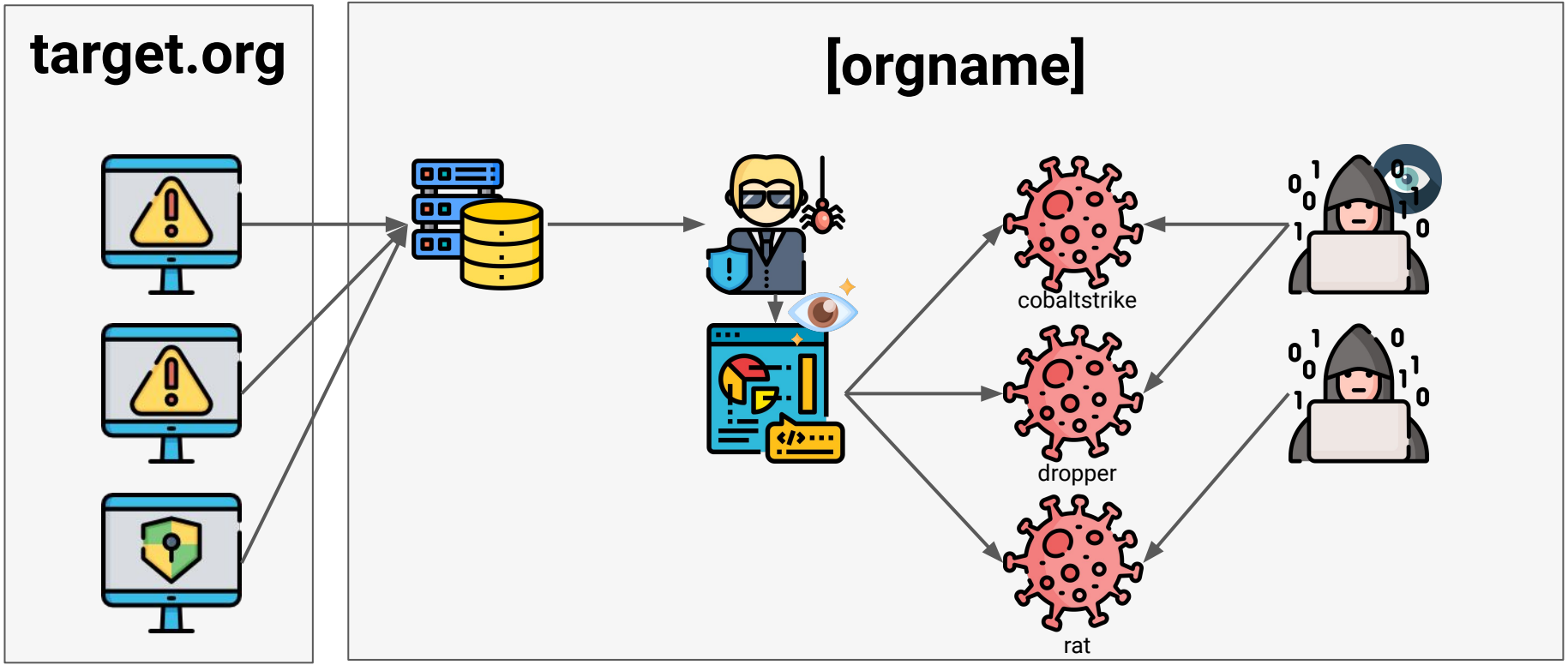
Organizacja pracy



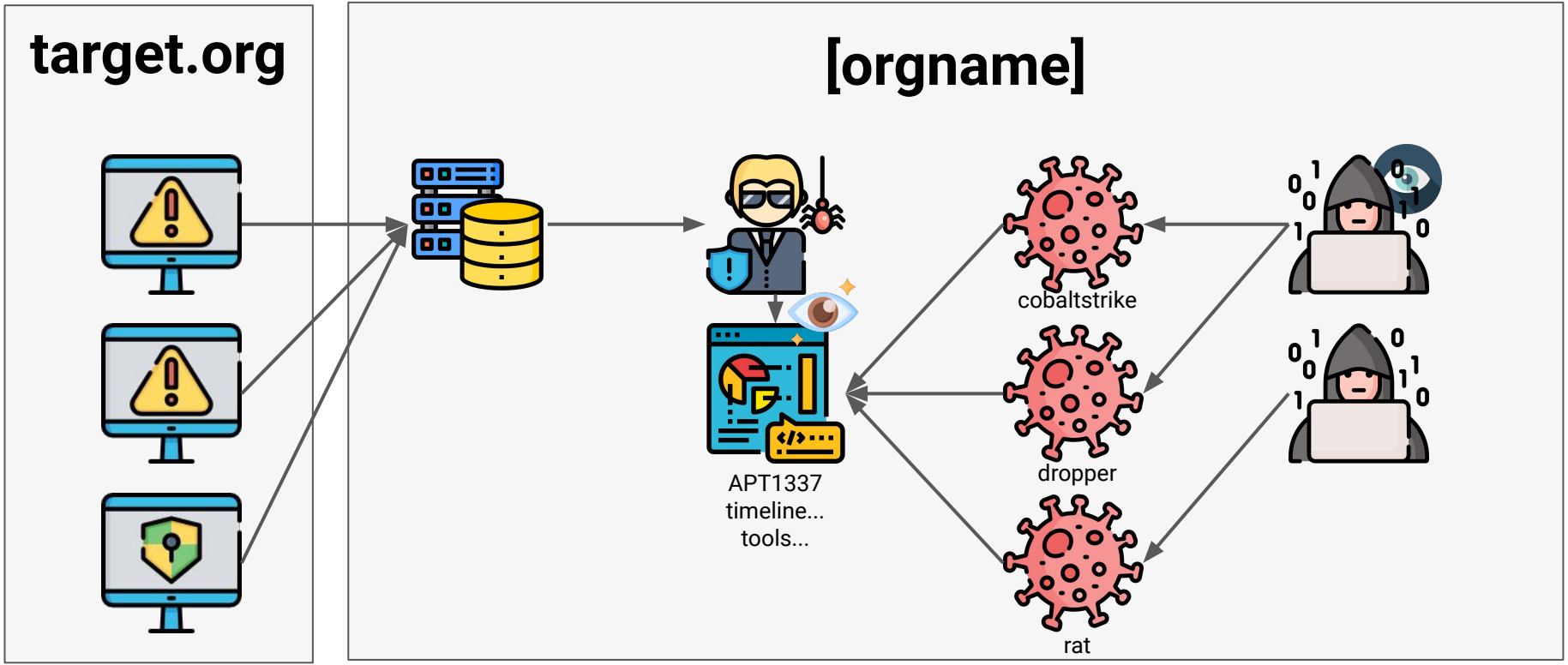
Organizacja pracy



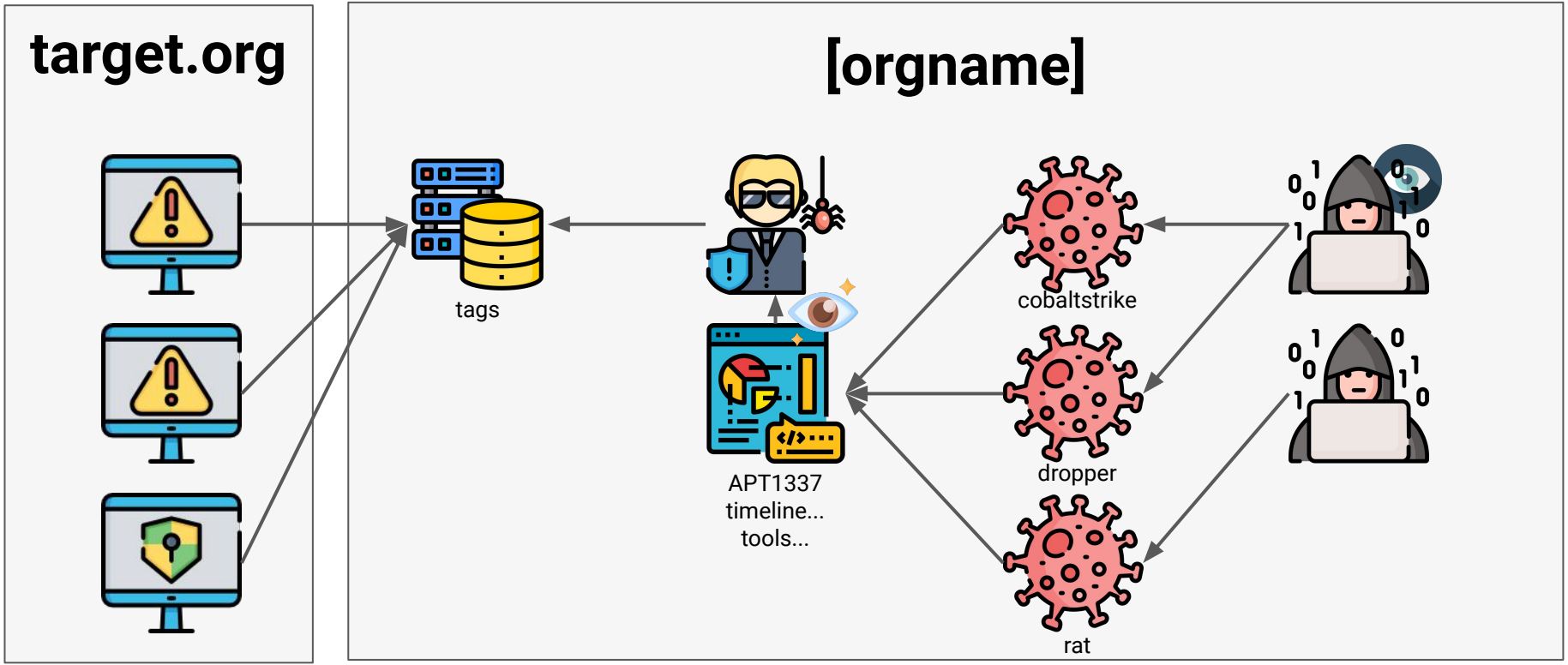
Organizacja pracy



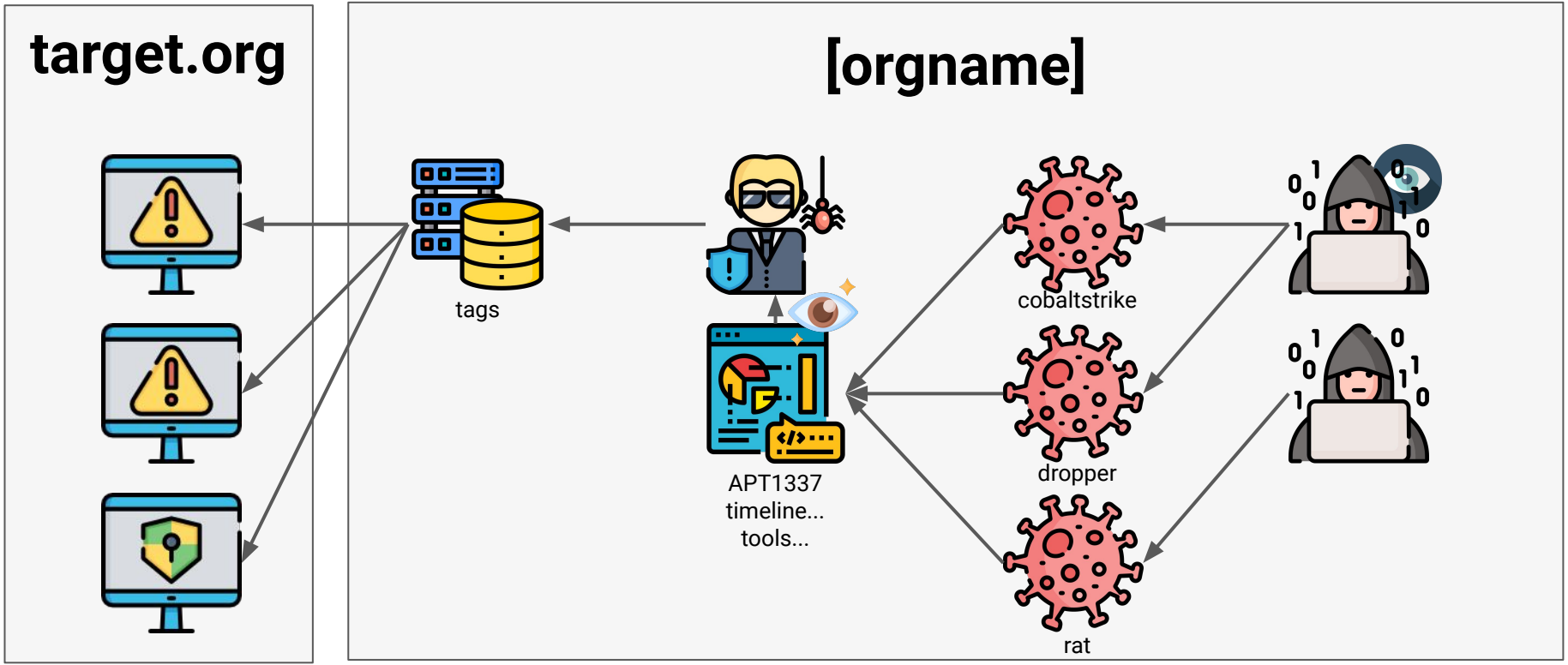
Organizacja pracy



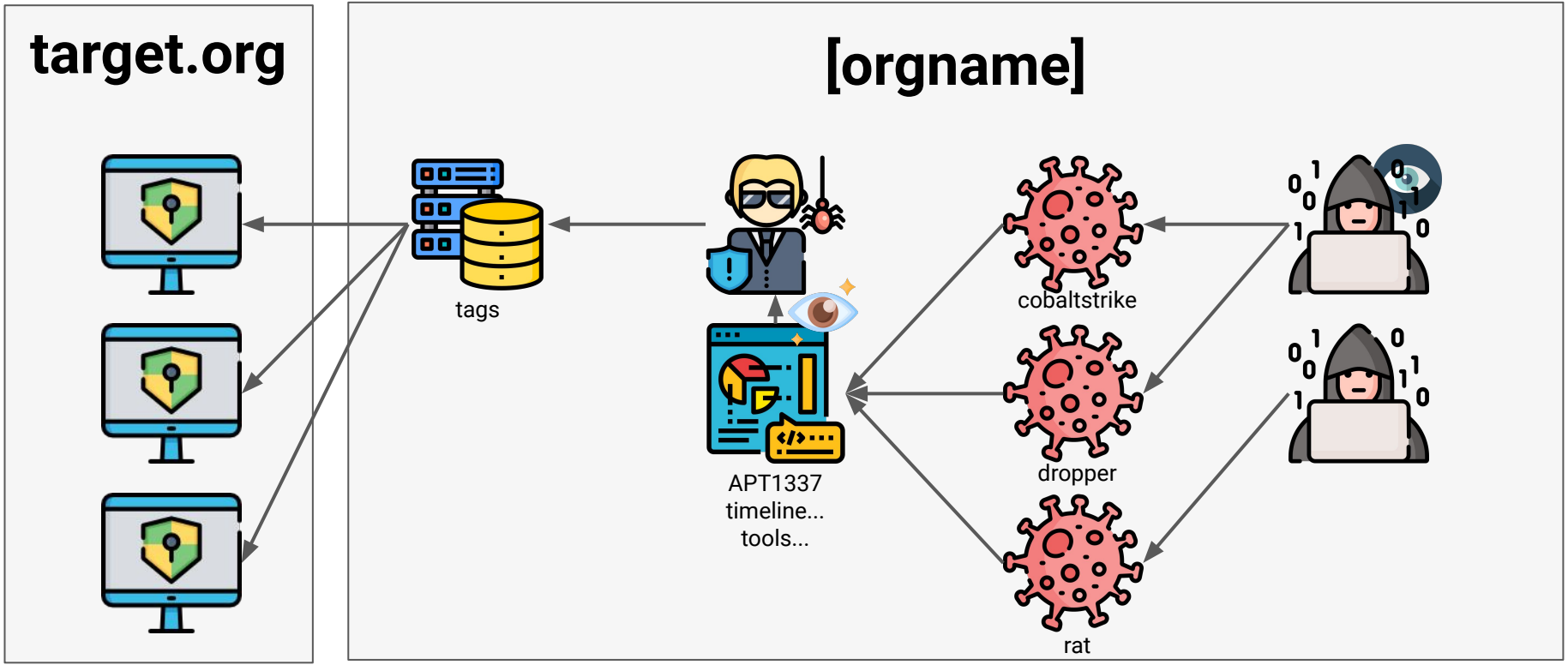
Organizacja pracy



Organizacja pracy



Organizacja pracy



Organizacja pracy

Dygresja

target.org

[o security.com

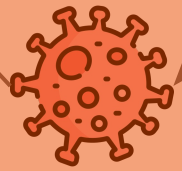
tags

APT1337
timeline...
tools...

analiza

cobaltstrike

dropper



rat

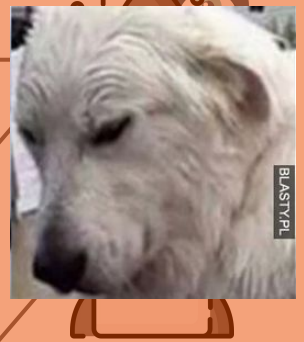
Organizacja pracy

Dygresja

target.org

[o security.com

symantec-enterprise-blogs.security.com



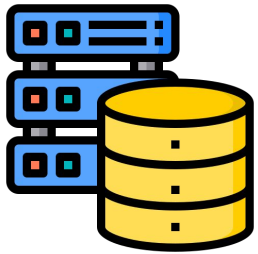
APT1337
timeline...
tools...

dropper

rat

analiza

Hunting



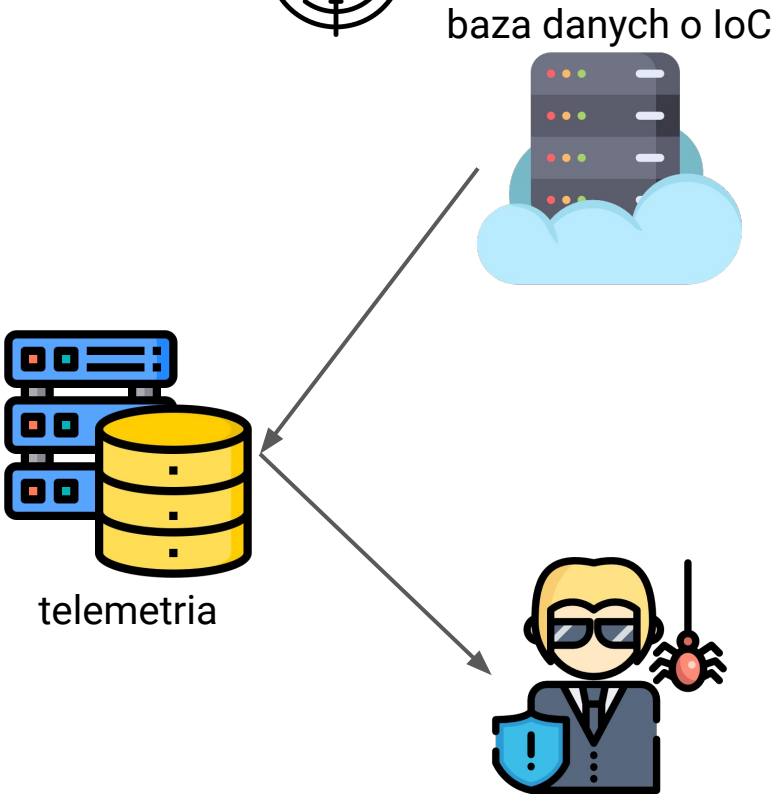
telemetria

Hunting

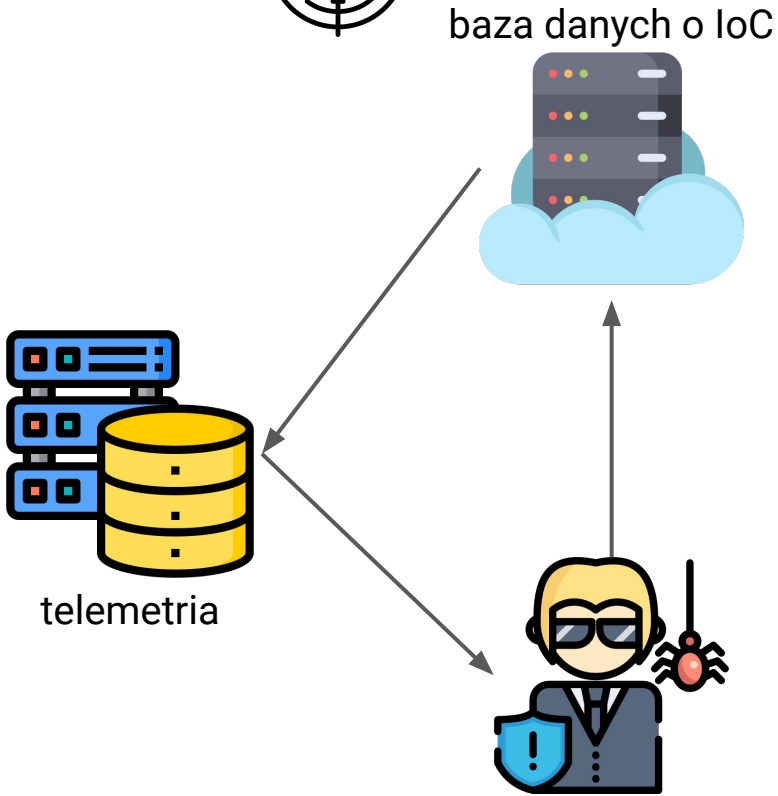
baza danych o IoC

telemetria

Hunting



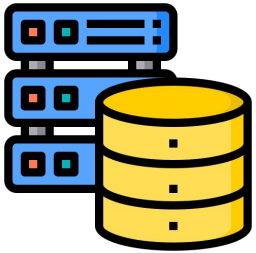
Hunting



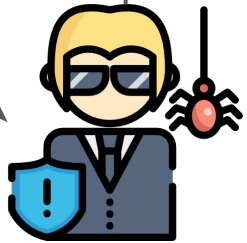
Hunting

baza danych o IoC

hashe, URLe, domeny
znalezione podczas analiz



telemetria

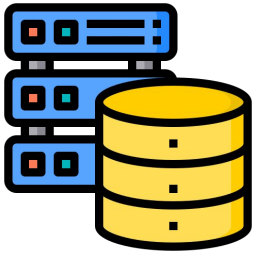


Hunting

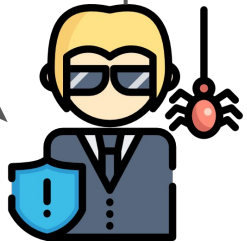
baza danych o IoC

hashe, URLe, domeny
znalezione podczas analiz

zewnętrzne i wewnętrzne
reguły yara



telemetria

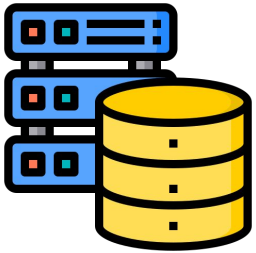


Hunting

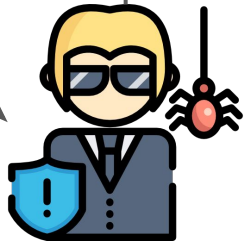
baza danych o IoC

hashe, URLe, domeny
znalezione podczas analiz

zewnętrzne i wewnętrzne
reguły yara

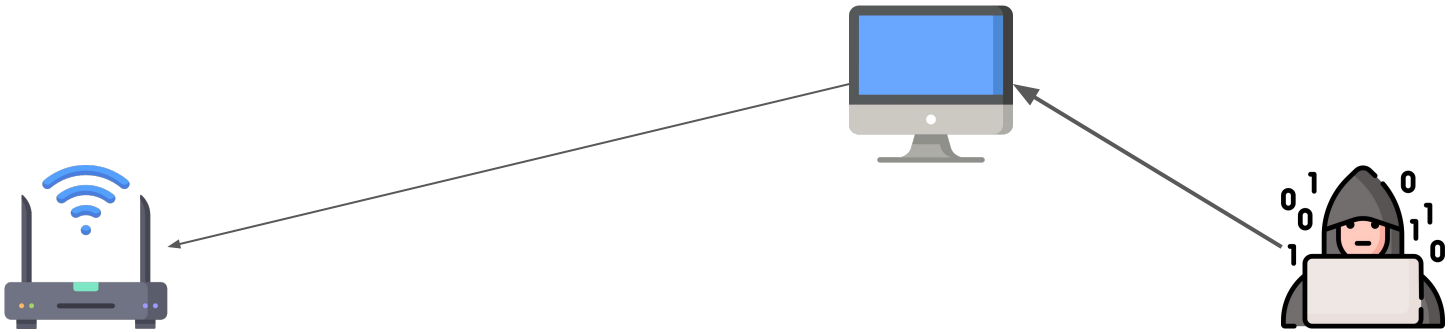


telemetria

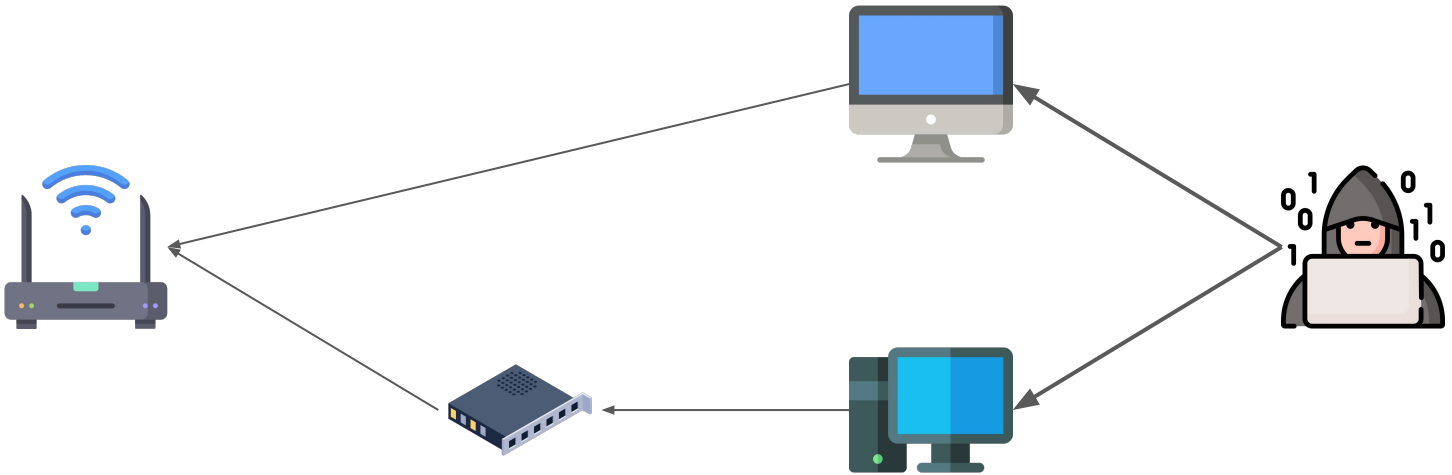


zewnętrzne raporty

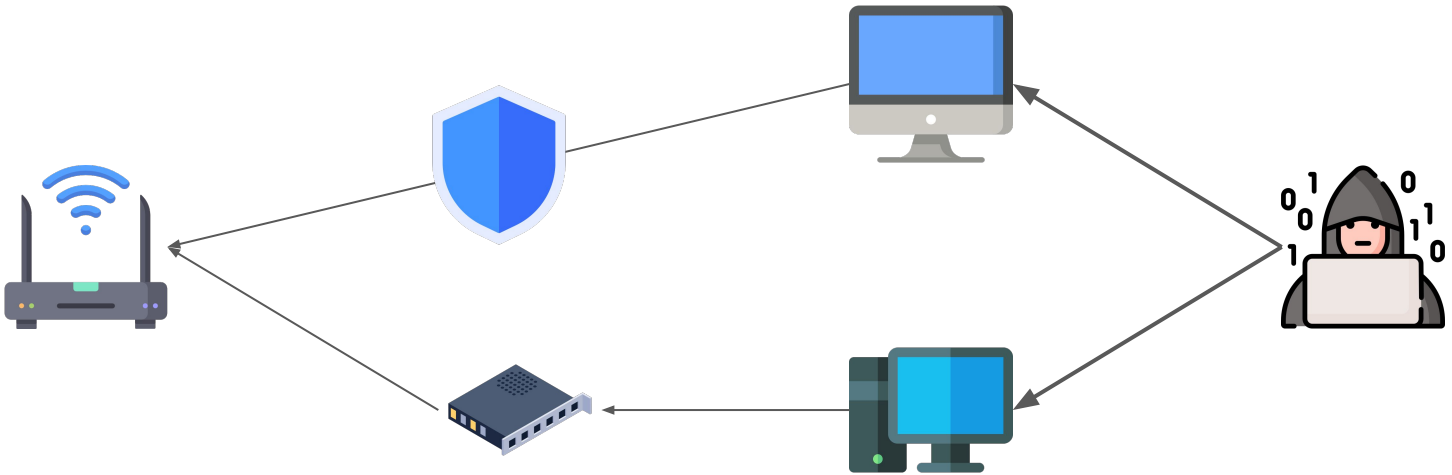
Środowisko pracy



Środowisko pracy

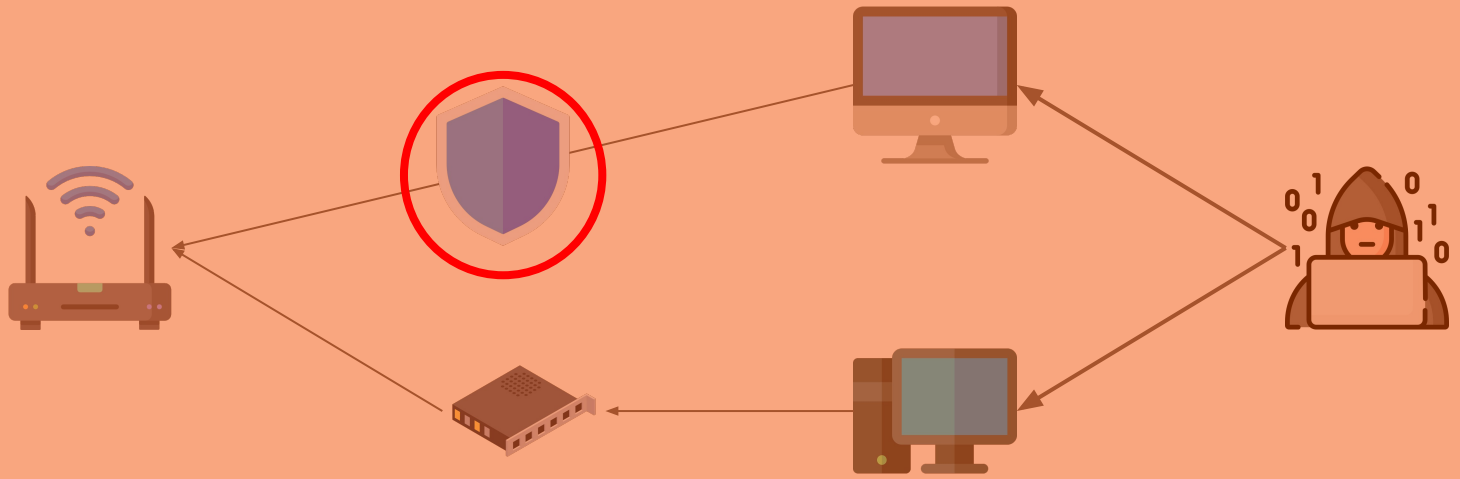


Środowisko pracy



Środowisko pracy

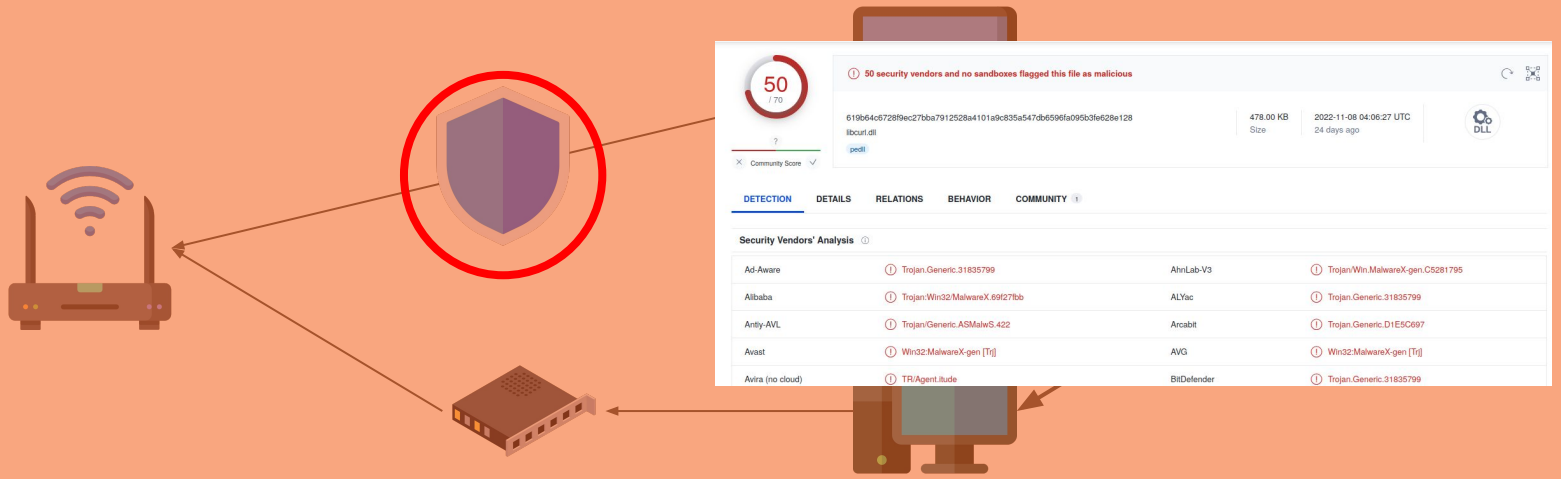
Dygresja



Czy wiesz że:
Wejście na stronę ładuje jej treść do pamięci przeglądarki?

Środowisko pracy

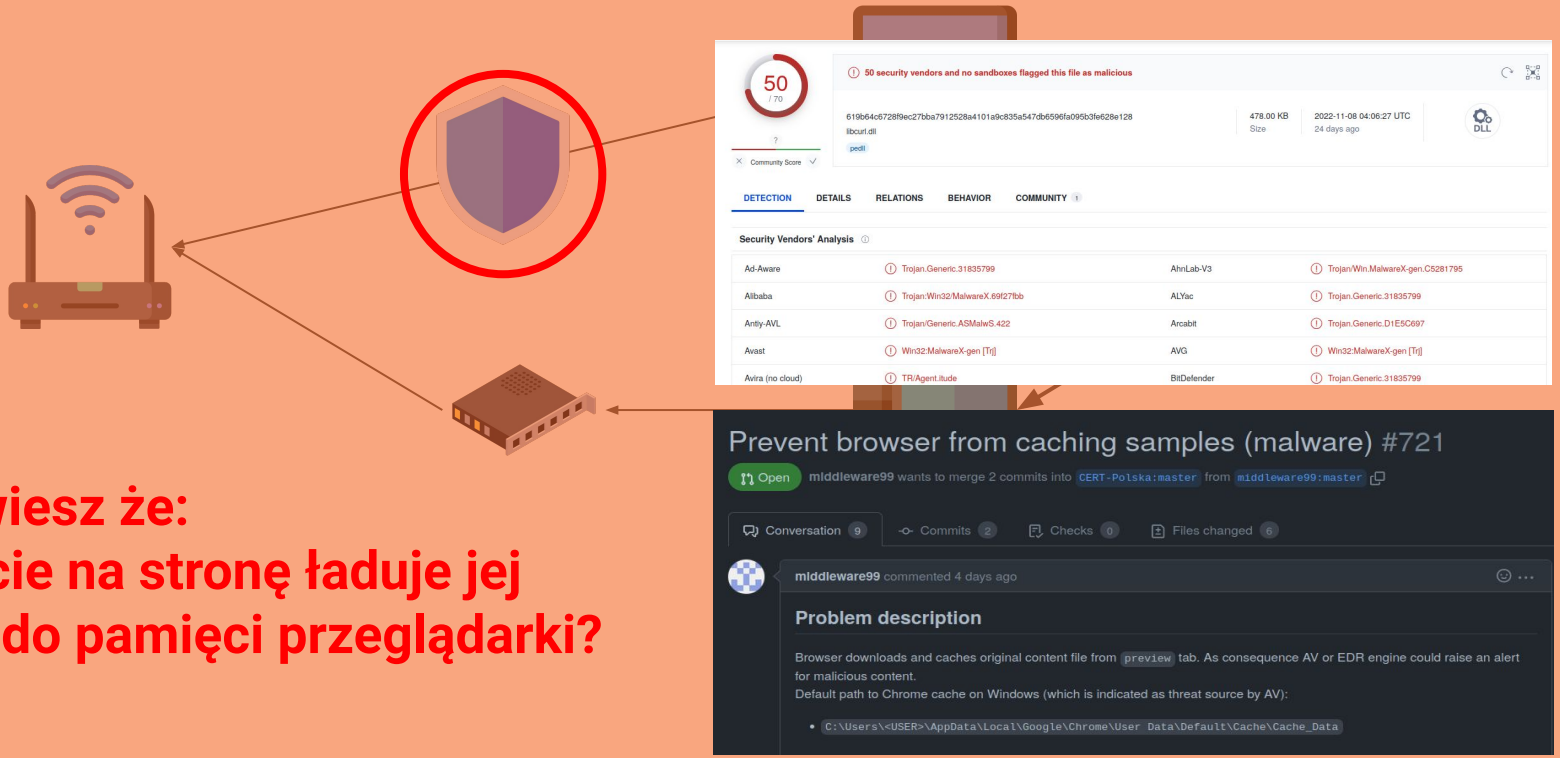
Dygresja



Czy wiesz że:
Wejście na stronę ładuje jej treść do pamięci przeglądarki?

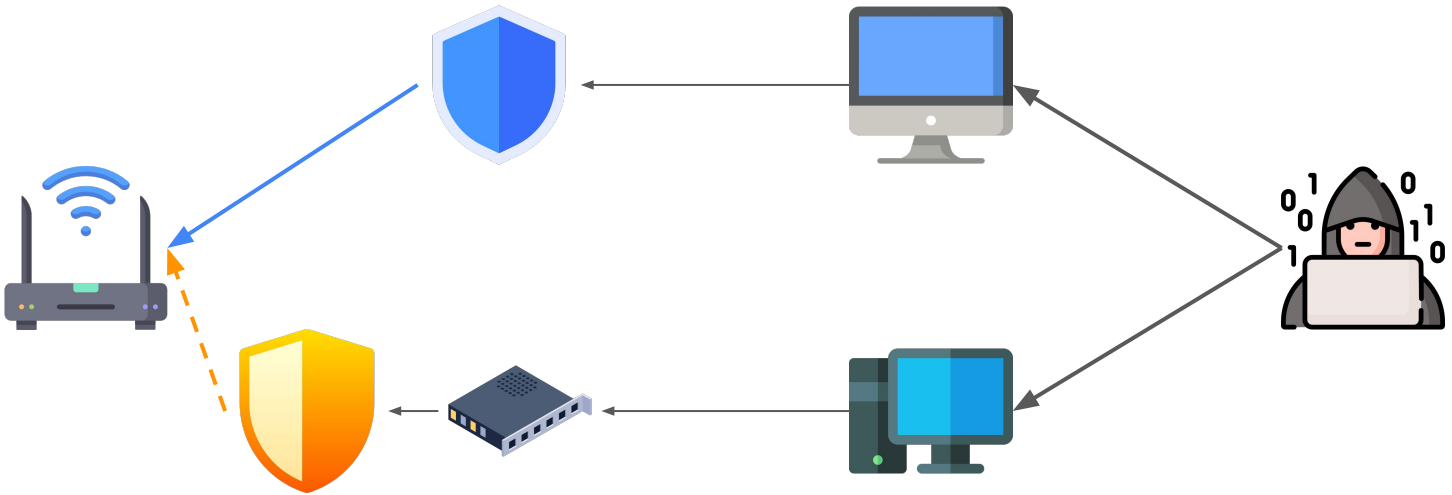
Środowisko pracy

Dygresja



Czy wiesz że:
Wejście na stronę ładuje jej treść do pamięci przeglądarki?

Środowisko pracy

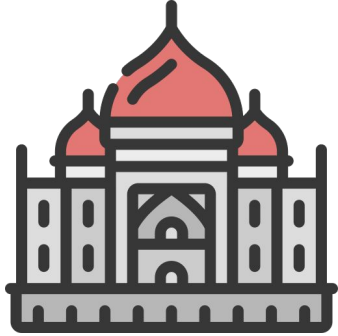


część 3

konkretnym przykładem

Case study

- Ministerstwo na bliskim wschodzie



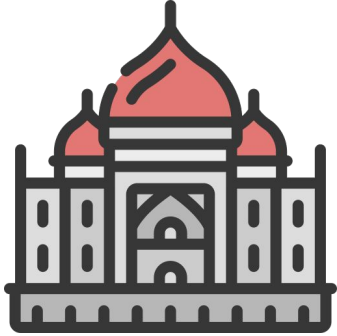
Case study

Dygresja

- Ministerstwo na bliskim wschodzie
- **ProxyShell** (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
- **ProxyLogon** (CVE-2021-26855, CVE-2021-27065)

ludzie, patchujcie się

Case study



- Ministerstwo na bliskim wschodzie
- **ProxyShell** (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
- **ProxyLogon** (CVE-2021-26855, CVE-2021-27065)
- Grupa zidentyfikowana później jako **Witchetty**
  - ...albo LookingFrog
  - ...wg. Eset, część TA410

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem
- 2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper.

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem
- 2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper.
- 2022-07-21: Dokładny skan sieci własnym narzędziem przypominającym nmap:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem
- 2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper.
- 2022-07-21: Dokładny skan sieci własnym narzędziem przypominającym nmap:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z backdoorem, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem
- 2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper.
- 2022-07-21: Dokładny skan sieci własnym narzędziem przypominającym nmap:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z backdoorem, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- 2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja proxy

Case study

- 2022-02-27: Zrzut pamięci LSASS:
  - rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full
- 2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)
- 2022-03-18: Atakujący używają s**dual use tool**Mimikatza żeby zrzucić hasła z pamięci
- 2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):
  - reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - **dual use tool**_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem
- 2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper
- 2022-07-21: Dokładny skan sieci własnym narzędziem prz**co tu reversować?**
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z backdoorem, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- 2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja proxy

Case study

- ~~2022-02-27: Zrzut pamięci LSASS:~~
  - ~~rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036 %profile%\public\dm.db full~~
- ~~2022-03-02: Skan domeny w celu znalezienia maszyn Windowsowych (Get-ADComputer)~~
- 2022-03-18: Atakujący używają swojego pseudo-Mimikatza żeby zrzucić hasła z pamięci
- ~~2022-04-29: Dokonanie zrzutu bazy SAM (Security Account Manager):~~
  - ~~reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive~~
- 2022-05-07: Instalacja backdoora LookBack (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- ~~2022-06-14: Znowu zrzut haseł z LSASS, tym razem prawdziwym Mimikatzem~~
- ~~2022-07-18: Ponowne użycie ProxyLogon, instalacja shella ChinaChopper.~~
- 2022-07-21: Dokładny skan sieci własnym narzędziem przypominającym nmap:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z backdoorem, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- 2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja proxy

Case study

- 2022-03-18: Atakujący używają swojego **pseudo-Mimikatza** żeby zrzucić hasła z pamięci
- 2022-05-07: Instalacja **backdoora LookBack** (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-07-21: Dokładny skan sieci własnym **narzędziem przypominającym nmap**:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z **backdoorem**, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- 2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja **proxy**

Case study

- ~~2022-03-18: Atakujący używają swojego **pseudo-Mimikatza** żeby zrzucić hasła z pamięci~~
- 2022-05-07: Instalacja **backdoora LookBack** (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- 2022-07-21: Dokładny skan sieci własnym **narzędziem przypominającym nmap**:
  - p.exe -l [IP_LIST] -p [PORT_LIST] -t 5
- 2022-07-28: Finalnie, dodanie scheduled taska z **backdoorem**, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- 2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja **proxy**

Case study

```
> ./malware.exe
[usage] :
    -h : PortScan Help.
    -l : ScanIP. Must be set ( 192.168.1.1 or 192.168.1.1/25)
    -p : ScanPort. ( default port : 445 )
    -t : Number of threads. ( The default number of threads is 5.)

[eg] :
    > PortScan.exe -l 192.168.1.1 -p 445 -t 5
```

Case study

- ~~2022-03-18: Atakujący używają swojego **pseudo-Mimikatza** żeby zrzucić hasła z pamięci~~
- 2022-05-07: Instalacja **backdoora LookBack** (i dodanie go jako scheduled taska):
  - rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init
- ~~2022-07-21: Dokładny skan sieci własnym **narzędziem przypominającym nmap**:~~
  - ~~p.exe -l [IP_LIST] -p [PORT_LIST] -t 5~~
- 2022-07-28: Finalnie, dodanie scheduled taska z **backdoorem**, który wykonał się za 3 dni:
  - rundll32 %programfiles%\internet explorer\systemcontrolmodel.dll, curl_share_init
- ~~2022-09-01: Ostatnia zaobserwowana aktywność - pobranie plików z dysku i instalacja **proxy**~~

Case study

619b64c6728f9ec27bba7912528a4101a9c835a547db6596fa095b3fe628e128

W sumie to wygląda jak libcurl.dll...

Case study

619b64c6728f9ec27bba7912528a4101a9c835a547db6596fa095b3fe628e128

W sumie to wygląda jak libcurl.dll...
...zaraz, co się dzieje w tym **curl_share_init**?

```
char *ptr = VirtualAlloc(0, 0x4f0, 0x1000, 0x40)
for (int i = 0; i < 0x4f0; i++) {
    ptr[i] = DATA[i];
}
some_function(ptr);
char *buffer = malloc(0x26c)
ptr(IMAGE_BASE, module_filename, address, LoadLibraryA);
```

Case study

Dygresja

619b64c6728f9ec27bba7912528a4101a9c835a547db6596fa095b3fe628e128

W sumie to wygląda jak libcurl.dll...
...zaraz, co się dzieje w tym **curl_share_init**?

```
char *ptr = VirtualAlloc(0, 0x4f0, 0x1000, 0x40)
for (int i = 0; i < 0x4f0; i++) {
    ptr[i] = DATA[i];
}
some_function(ptr);
char *buffer = malloc(0x26c)
ptr(IMAGE_BASE, module_filename, address, LoadLibraryA);
```

Case study

```
sbox, perm, j = .....
out = []
k = 0
for i in range(len(data)):
    j = sbox[i % 256]
    k = (k + j + i) % 256
    tmp = sbox[k]
    sbox[k] = j
    sbox[i % 256] = tmp
    out.append(data[i] ^ sbox[tmp ^ j])
```

Case study

Dygresja

```
sbox, perm, j = .....
out = []
k = 0
for i in range(len(data)):
    j = sbo
    tmp = sbox[k]
    sbox[k] = j
    sbox[i % 256] = tmp
    out.append(data[i] ^ sbox[tmp ^ j])
```

gdybym dostawał złotówkę

za każdego odpakowanego cobaltstrike...

Case study

- Deszyfrowanie shellcode...
  - Kod który zawsze wygląda tak samo, mimo że zawsze wygląda inaczej.
  - Jakieś xory, shifty, rc4, podmiany słowników

Case study

- Deszyfrowanie shellcode...
  - Kod który zawsze wygląda tak samo, mimo że zawsze wygląda inaczej.
  - Jakieś xory, shifty, rc4, podmiany słowników
- Po odpakowaniu, wygląda już lepiej
  - "Kiedyś już coś takiego widziałem"
  - SodomBodyLoad
  - https://threatgen.com/taking-a-closer-look-at-the-lookback-malware-campaign-part-1/

Case study

- Deszyfrowanie shellcode...
  - Kod który zawsze wygląda tak samo, mimo że zawsze wygląda inaczej.
  - Jakieś xory, shifty, rc4, podmiany słowników
- Po odpakowaniu, wygląda już lepiej
  - "Kiedyś już coś takiego widziałem"
  - SodomBodyLoad
  - https://threatgen.com/taking-a-closer-look-at-the-lookback-malware-campaign-part-1/
- But wait, there's more...

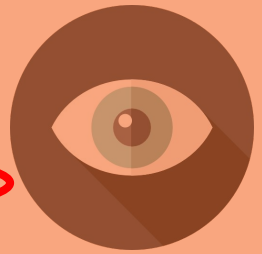
Case study

3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042

Nieznane wcześniej narzędzie odkryte po analizie poprzedniej próbki.
Początkowo znany jedynie hash, po kilku dniach udało się uzyskać plik.

Case study

Dygresja



3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042

Nieznane wcześniej narzędzie odkryte po analizie poprzedniej próbki.
Początkowo znany jedynie hash, po kilku dniach udało się uzyskać plik.

Nie ma na VT, przykro mi :).

Case study

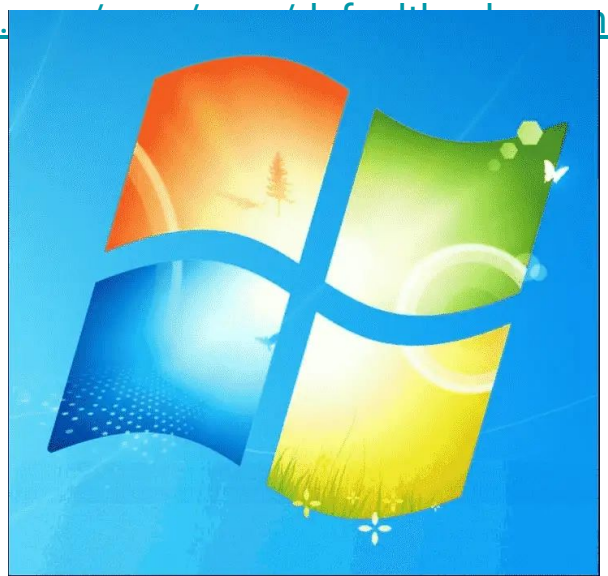
3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042

Nieznane wcześniej narzędzie odkryte po analizie poprzedniej próbki.
Początkowo znany jedynie hash, po kilku dniach udało się uzyskać plik.
Pobiera bitmapę spod adresu [redacted]
https://raw.githubusercontent.com/xxxx/xxxx/defaultbackground.bmp

Case study

3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042

Nieznane wcześniej narzędzie odkryte po analizie poprzedniej próbki.
Początkowo znany jedynie hash, po kilku dniach udało się uzyskać plik.
Pobiera bitmapę spod adresu [redacted]
https://raw.githubusercontent.[redacted]d.bmp



Case study

Dygresja

3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042

Nieznane wcześniej narzędzie odkryte po analizie poprzedniej próbki.
Początkowo znany jedynie hash, po kilku dniach udało się uzyskać plik.
Pobiera bitmapę spod adresu
https://raw.githubusercontent.[redacted]d.bmp

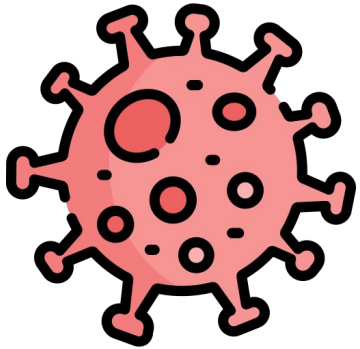
Wersja na blogu po przejściu przez stratny round-trip bmp -> jpg -> bmp

Case study

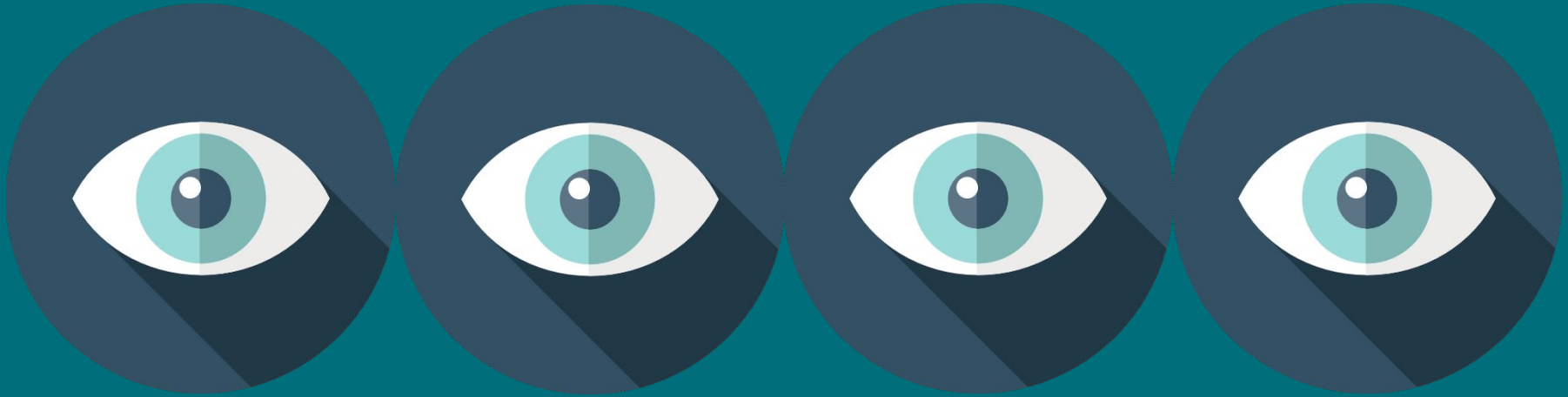
decrypted payload (hash niepubliczny)

Customowy backdoor jak to backdoor:

- Tworzenie i usuwanie folderów
- Zarządzanie plikami
- Zarządzanie procesami
- Zarządzanie rejestrem
- Startowanie procesów
- Pobieranie aktualizacji



część 4



podsumowaniem

Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora LookBack
- Nowy, nieużywany wcześniej backdoor używający steganografii w bmp

Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora LookBack
- Nowy, nieużywany wcześniej backdoor używający steganografii w bmp
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzystencji
- Własna alternatywa dla mimikatza

Podsumowując

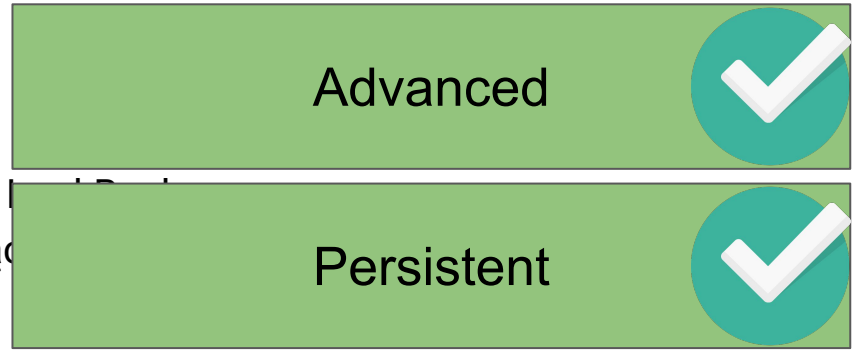
- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora LookBack
- Nowy, nieużywany wcześniej backdoor używający steganografii w bmp
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzystencji
- Własna alternatywa dla mimikatza

Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora LookBack
- Nowy, nieużywany wcześniej backdoor używający steganografii w bmp
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzystencji
- Własna alternatywa dla mimikatza
- Wszystko trwało ponad pół roku.

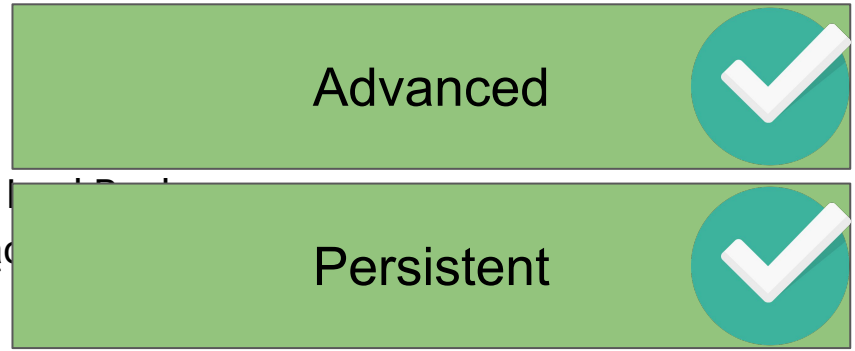
Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora
- Nowy, nieużywany wcześniej backdoor używając
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzystencji
- Własna alternatywa dla mimikatza
- Wszystko trwało ponad pół roku.



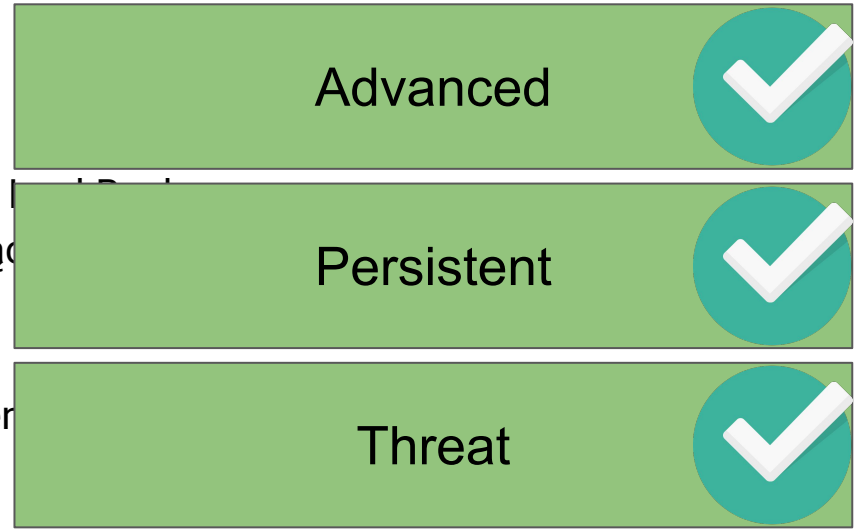
Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora
- Nowy, nieużywany wcześniej backdoor używając
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzystencji
- Własna alternatywa dla mimikatza
- Wszystko trwało ponad pół roku.
- ...I działo się w ministerstwie na bliskim wschodzie



Podsumowując

- Wejście do organizacji za pomocą eksploitów
- Kilka wersji znanego już poprzednio backdoora
- Nowy, nieużywany wcześniej backdoor używając
- Nowe, własne proxy
- Nowy, własny skaner sieci
- Nowe mikro-narzędzie do zachowania perzyster
- Własna alternatywa dla mimikatza
- Wszystko trwało ponad pół roku.
- ...I działo się w ministerstwie na bliskim wschodzie



Są też inne

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor

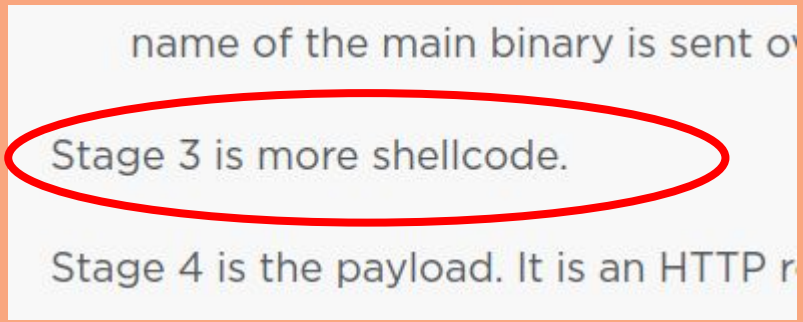
Są też inne

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer

Są też inne

Dygresja

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer



Są też inne

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer
- Daxin: Zaawansowane proxy od chińskiej grupy APT
  - Feat: Sterownik hookujący stos sieciowy Windowsa w celu bardzo cichej komunikacji

Są też inne

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer
- Daxin: Zaawansowane proxy od chińskiej grupy APT
  - Feat: Sterownik hookujący stos sieciowy Windowsa w celu bardzo cichej komunikacji
- Cranefly: RPC-over-IIS logs
  - Feat: Sprytny backdoor który komendy od operatora czyta z logów IIS

Są też inne

- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer
- Daxin: Zaawansowane proxy od chińskiej grupy APT
  - Feat: Sterownik hookujący stos sieciowy Windowsa w celu bardzo cichej komunikacji
- Cranefly: RPC-over-IIS logs
  - Feat: Sprytny backdoor który komendy od operatora czyta z logów IIS
- Tysiąc próbek CobaltStrike, każda spakowana innym własnym packerem

Są też inne

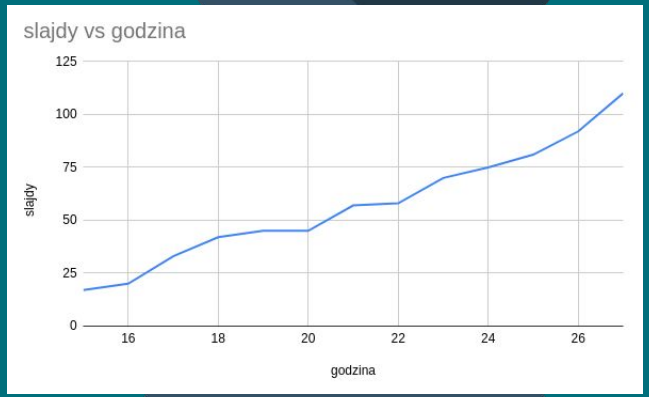
- Billbug: Ataki na CA i instytucje rządowe w Azji
  - Feat: bardzo uparty backdoor
- Stonefly: Exploit na log4j, eksfiltracja danych z całej organizacji w ciągu 3 dni
  - Feat: RAT z 4 warstwami obfuskacji, własny infostealer
- Daxin: Zaawansowane proxy od chińskiej grupy APT
  - Feat: Sterownik hookujący stos sieciowy Windowsa w celu bardzo cichej komunikacji
- Cranefly: RPC-over-IIS logs
  - Feat: Sprytny backdoor który komendy od operatora czyta z logów IIS
- Tysiąc próbek CobaltStrike, każda spakowana innym własnym packerem
  - Poważnie, nie mogę już patrzeć na CobaltStrike

Co z tego wynika? 🤔

Q&A?

msm@tailcall.net

@MsmCode



Icons from flaticon.com by freepik, phatplus, juicy_fish - thanks!