SECURITY DAYS

STRACH Z NEZNÁMEHO, TO JE ZERO-DAY. AKO SI MÔŽEM POMÔCŤ

Július Selecký

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

Prečo by ma to malo zaujímať?

- Kybernetické útoky
  - obrovské náklady pre spoločnosti
  - strata dát
  - poškodenie dobrého mena

- Zero-Day hrozby, APT (pokročilé pretrvávajúce útoky)
- Dynamické prostredie

V čom je problém?

- Obmedzené výpočtové zdroje pre koncové body
- LiveGrid poskytuje dodatočnú ochranu pre ESET Endpoint
- ESET Endpoint a LiveGrid chránia pred známymi hrozbami

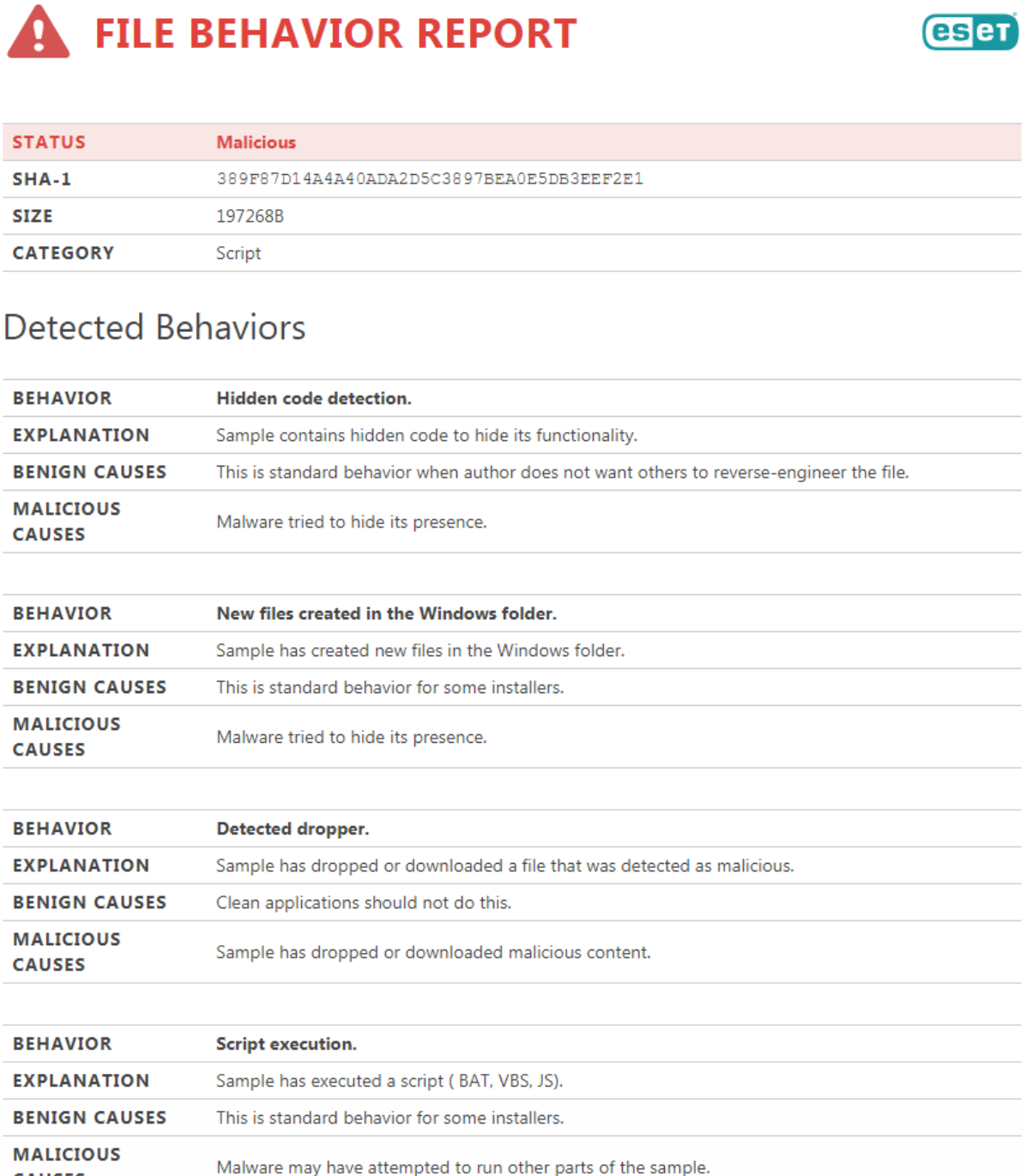
Takže...

- Neznáme či podozrivé súbory by mali byť počas analýzy zablokované
- Na detekciu podozrivých a škodlivých súborov je nevyhnutná kompletná analýza správania

ESET DYNAMIC THREAT DEFENSE

Čo robí EDTD?

- EDTD ako ďalšia vrstva zabezpečenia po Endpoint Security
- Hybridný cloudový sandbox
- Využívanie strojového učenia
- Okamžitá ochrana pre všetky počítače
- Podrobný report



FILE BEHAVIOR REPORT

STATUS	Malicious
SHA-1	389F87D14A4A40ADA2D5C3897BEA0E5DB3EEF2E1
SIZE	197268B
CATEGORY	Script

Detected Behaviors

BEHAVIOR	**Hidden code detection.**
EXPLANATION	Sample contains hidden code to hide its functionality.
BENIGN CAUSES	This is standard behavior when author does not want others to reverse-engineer the file.
MALICIOUS CAUSES	Malware tried to hide its presence.

BEHAVIOR	**New files created in the Windows folder.**
EXPLANATION	Sample has created new files in the Windows folder.
BENIGN CAUSES	This is standard behavior for some installers.
MALICIOUS CAUSES	Malware tried to hide its presence.

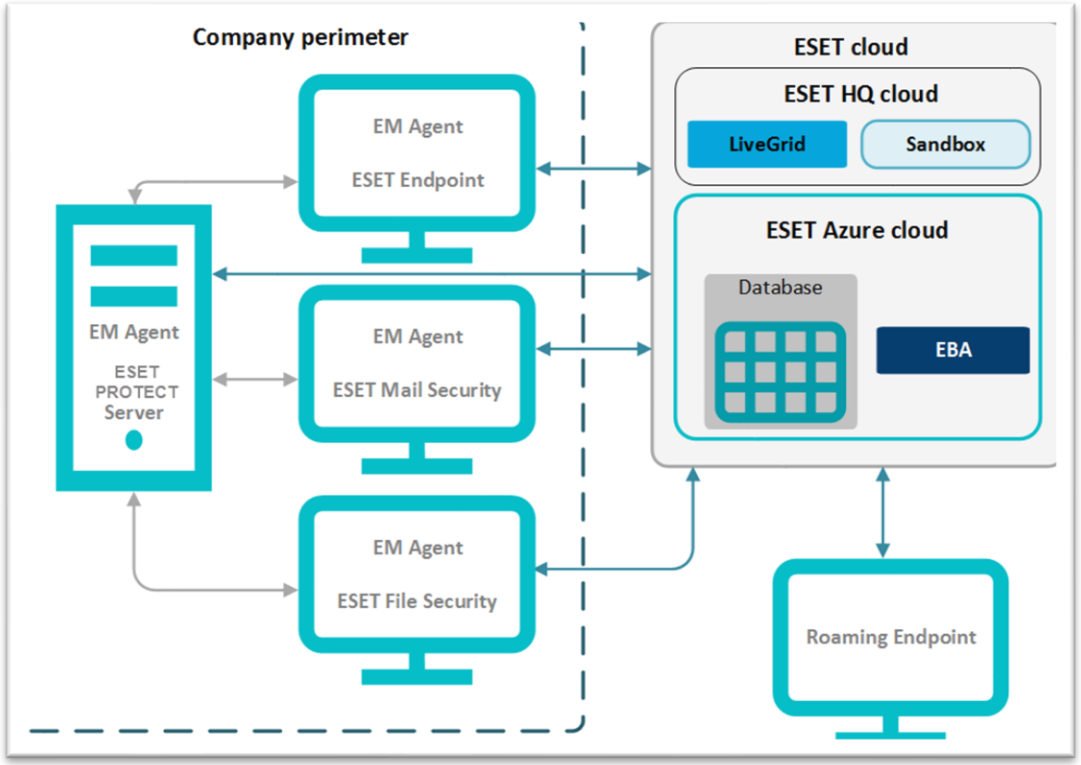
BEHAVIOR	**Detected dropper.**
EXPLANATION	Sample has dropped or downloaded a file that was detected as malicious.
BENIGN CAUSES	Clean applications should not do this.
MALICIOUS CAUSES	Sample has dropped or downloaded malicious content.

BEHAVIOR	**Script execution.**
EXPLANATION	Sample has executed a script (BAT, VBS, JS).
BENIGN CAUSES	This is standard behavior for some installers.
MALICIOUS CAUSES	Malware may have attempted to run other parts of the sample.

ESET DYNAMIC THREAT DEFENSE

Ako EDTD funguje?

- Odoslanie vzorky do ESET Cloud
- Spúšťanie a testovanie vzorky v sandboxe
- Blokovanie súboru a report



Kľúčové benefity

- Cloudová technológia schopná analyzovať súbory za menej ako päť minút
- Dôležitá bezpečnostná vrstva chrániaca koncové body a poštu pred novými pokročilými hrozbami
- Jednoduché nastavenie (agentless) a správa z centrálnej konzoly ESET PROTECT (ESMC)
- Analýza súborov stiahnutých z webu, emailových správ, komprimovaných súborov či súbory z vymeniteľných médií

Spolupráca s ESET produktami

- ESET Mail Security (verzia 7+)
- ESET Endpoint Antivirus/Security (verzia 7+)
- ESET File Security (verzia 7+)

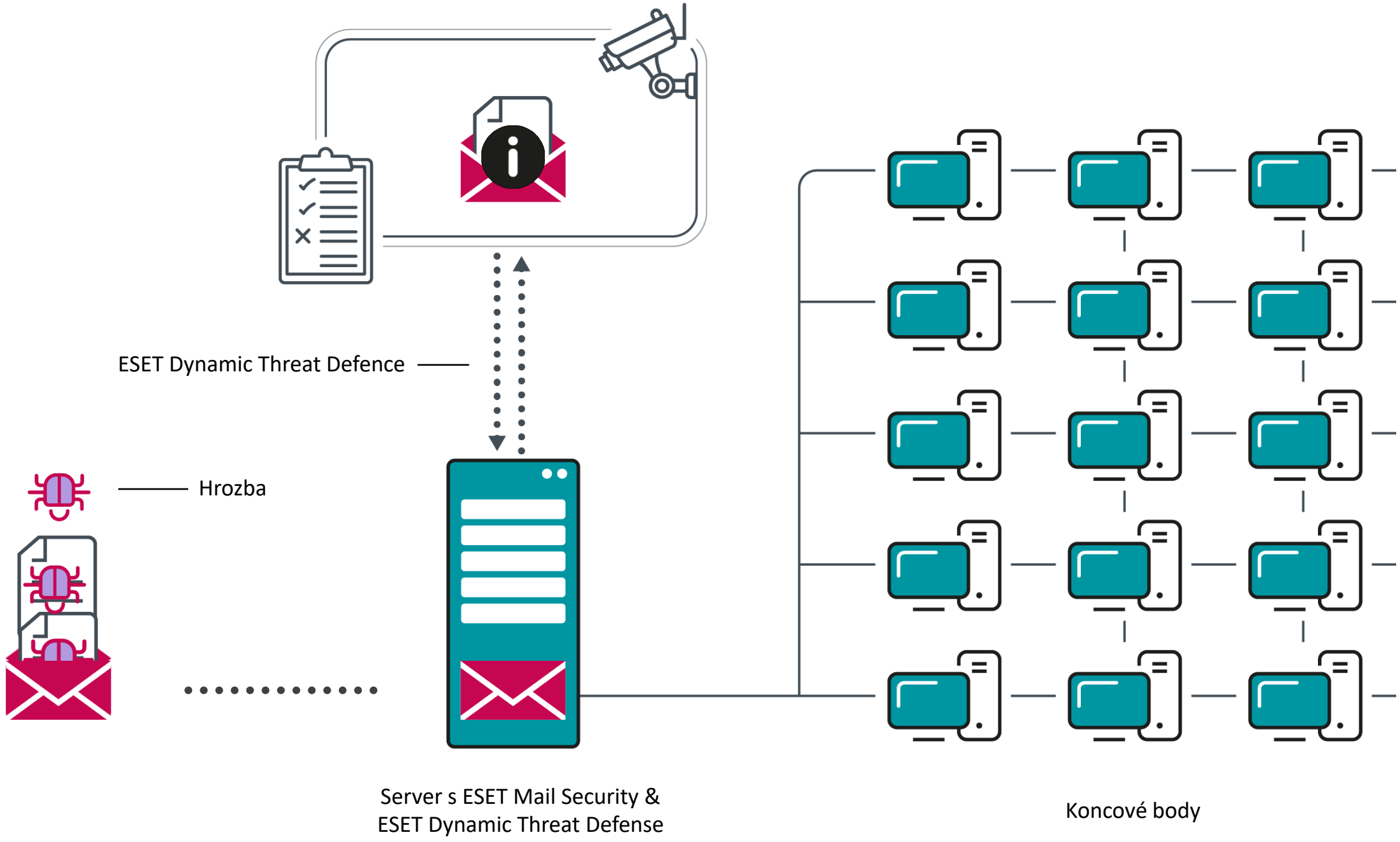
Phishing správy s malvérom

Bezpečná sieť

Začiatok

Koniec

Ukradnuté alebo zašifrované dáta


ESET Dynamic Threat Defence
Hrozba
Server s ESET Mail Security &
ESET Dynamic Threat Defense
Koncové body

Phishing správy s malvérom

Bezpečná sieť

Koniec

Začiatok

Malvér cez USB alebo sociálne inžinierstvo

Ukradnuté alebo zašifrované dáta

Neznámy malvér odstránený v priebehu 5 minút, namiesto niekoľkých týždňov/mesiacov!

Pracovná stanica s ESET Endpoint technológiou & ESET Dynamic Threat Defense

ESET Dynamic Threat Defense

Je to bezpečné?

- Dátové centrum v Bratislave priamo v ESETe
- Žiadne analýzy či vzorky pre tretie strany
- Odstránenie vzoriek zo serverov ESET
- Vylúčenia (typy súborov, priečinky, procesy, hash)
- Nastavenie maximálnej doby čakania
- Globálna databáza ukladá hash hodnoty

Privítajte prvotriednu bezpečnosť

- Homeoffice ready
- Čarovné riešenie? ☺ Nie...
- Prečo som o tejto technológií nepočul?
  - Cloudový sandbox - mainstream
  - Vyvinuté pre Enterprise dostupné aj pre SMB

ESET Dynamic Threat Defense (EDTD) v produktových balíkoch

Cloudové produktové balíky

- PROTECT ADVANCED
- PROTECT COMPLETE
- PROTECT ENTERPRISE
- PROTECT MAIL PLUS

On-prem produktové balíky

- PROTECT ENTERPRISE ON-PREM
- PROTECT COMPLETE ON-PREM
- PROTECT ADVANCED ON-PREM

Skúšobná licencia

ESET PROTECT ADVANCED pre 25 endpointov na 30 dní
- aktivácia cez ESET Business Account (EBA)

V prípade otázok kontaktujte:

- ESET obchodný kontakt
- ESET partnera
- obchod@eset.sk

SECURITY DAYS

Ďakujem za pozornosť

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE