

# Porazte kyberzločin vďaka jasným a praktickým informáciám

## Problém

Kybernetickí zločinci nie sú len náhodní útočníci. Sú organizovaní, vytrvalí a neustále vyvíjajú svoje taktiky s cieľom **maximalizovať vplyv a zisk**. Či už ide o ransomérové kartely alebo infostealery, mnohé skupiny v súčasnosti fungujú ako agilné a technicky vyspelé globálne podniky s jasne vymedzenými úlohami a medzinárodným dosahom. **Príjmy z ransoméru neustále rastú**, keďže vydieranie je čoraz cielenejšie a agresívnejšie. Bezpečnostné tímy tak musia mať k dispozícii viac než len jednoduché indikátory narušenia bezpečnosti. Potrebujú **komplexné a kontextuálne informácie** o tom, ako tieto skupiny fungujú, o čo im ide a ako ich zastaviť skôr, než spôsobia skutočné škody.

**256 DNÍ**

priemerný čas, za ktorý sa organizácia úplne zotaví z útoku ransoméru

Zdroj: Forrester: metriky o útokoch ransoméru za rok 2024 (podľa odvetvia)

**50 %**

medziročný nárast útokov ransoméru (2025)

Zdroj: Analýzy spoločnosti ESET o stránkach s uniknutými údajmi

**15 % DEŠTRUKTÍVNEJŠIE**

ransomérové útoky v porovnaní s inými typmi útokov

Zdroj: Forrester: metriky o útokoch ransoméru za rok 2024 (podľa regiónu)

## Riešenie

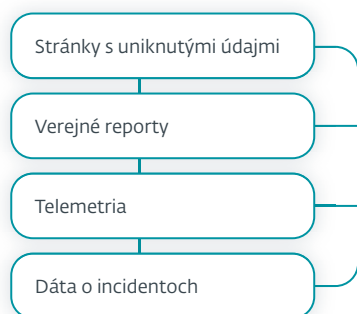
### REPORTY ESET THREAT INTELLIGENCE O KYBERZLOČINE

Reporty ESET Threat Intelligence o kyberzločine (eCrime Reports) ponúkajú len **praktické informácie** bez akýchkoľvek nadbytočností. Každý report vám poskytne jasný obraz o tom, **ako fungujú kyberzločinecké skupiny** – od používaných nástrojov cez infraštruktúru až po monetizačné taktiky. Získate poznatky, ktoré vám pomôžu narušiť ich operácie, nielen odhaliť malvér. Tieto informácie, podporené globálnymi výskumnými tímami spoločnosti ESET, sú založené na reálnej telemetrii, hĺbkovej technickej analýze a priamom monitorovaní nekalých aktivít. Reporty neponúkajú len dáta, ale aj **strategickú výhodu**.

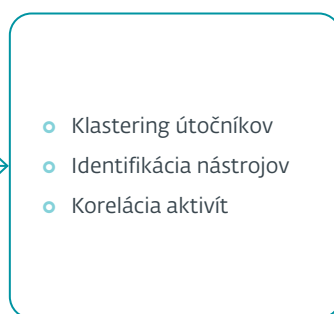
### AKO TO FUNGUJE?

Namiesto toho, aby sme sa zameriavali na známe skupiny RaaS a všeobecné prehľady, rozoberáme samotných operátorov – skutočných zločincov, ktorí stoja za útokmi.

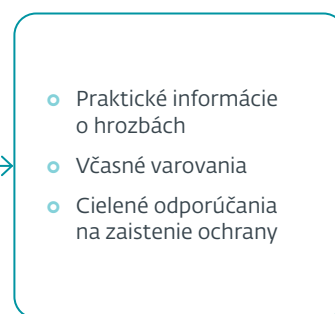
#### ZDROJE ÚDAJOV



#### ANALÝZA



#### VÝSTUPY



### V ČOM SÚ REPORTY O KYBERZLOČINE SPOLOČNOSTI ESET INÉ

#### Proaktívna ochrana

Získajte informácie nielen o kyberzločineckých skupinách, ale aj o operátoroch, ktorí útoky skutočne vykonávajú. Zistíte, ako fungujú, aby ste mohli predvídať, o čo sa pokúsia najbližšie – a buďte o krok vpred.

#### Prevádzková efektívnosť

Oprite sa o jasné, dôkladne spracované poznatky zo skutočných incidentov bez zbytočných informácií. Uľahčíte svojmu tímu odhaľovanie hrozieb, reagujte rýchlejšie a zamerajte sa na ich hľadanie tam, kde je to najdôležitejšie.

#### Bezkonkurenčný prehľad

Choďte nad rámec verejných kanálov o hrozbách a získajte komplexnejší prehľad o monetizačných taktikách, infraštruktúre a správaní operátorov v praxi – to všetko s podporou globálnej telemetrie a výskumu spoločnosti ESET.

# Čo obsahujú reporty ESET Threat Intelligence o kyberzločine

Typ prístupu	Obsah reportov	eCrime Reports	eCrime Reports Advanced
<p>MESAČNE</p> <p><b>Súhrn aktivity</b></p>	<ul style="list-style-type: none"> <li>Najnovšie kampane ransomvéru a infostealeroz spracované do prehľadných strategických informácií</li> <li>Kto je terčom útokov, ako prebiehajú, čo sa pokazilo</li> <li>Kľúčové poznatky, indikátory IOC a usmernenia na posilnenie ochrany</li> </ul>	✓	✓
<p>PERIODICKY</p> <p><b>Technická analýza</b></p>	<ul style="list-style-type: none"> <li>Dôkladný prehľad o konkrétnych útočníkoch (napr. FIN7)</li> <li>Úplný reťazec útoku od počítačného prístupu po krádež údajov</li> <li>Taktiky a nástroje útočníkov, využívaná infraštruktúra, mapovanie MITRE ATT&amp;CK®, indikátory IOC</li> </ul>	✓	✓
<p>MESAČNE</p> <p><b>Mesačný súhrn</b></p>	<ul style="list-style-type: none"> <li>Prehľad nedávnej aktivity ransomvéru/infostealeroz pripravený pre vedúcich pracovníkov</li> <li>Kľúčové trendy, významné incidenty, novovznikajúce hrozby</li> <li>Pomáha vedeniu posúdiť riziko a stanoviť priority bez technickej zložitosti</li> </ul>	✓	✓
<p><b>Informačný kanál o kyberzločine</b></p>	<ul style="list-style-type: none"> <li>Najnovšie a dôkladne spracované indikátory IOC o ransomvérových gangoch, ich operátoroch a kampaniach infostealeroz</li> <li>K dispozícii v štandardnom formáte STIX/TAXII</li> </ul>	✓	✓
<p><b>ESET AI Advisor</b></p>	<ul style="list-style-type: none"> <li>Využíva poznatky o kyberzločine na zodpovedanie otázok týkajúcich sa hrozieb</li> <li>Pomáha interpretovať incidenty a správanie útočníkov</li> <li>Okamžite tímom a pracovníkom na rozhodujúcich pozíciách sprístupňuje informácie o hrozbách</li> </ul>	X	✓
<p><b>Prístup k serveru MISIP</b></p>	<ul style="list-style-type: none"> <li>Priama integrácia s dôkladne spracovanými informáciami o hrozbách</li> <li>Automatické zhromažďovanie indikátorov IOC na zvýšenie ochrany</li> <li>Zjednodušenie postupov, urýchlenie detekcie a podpora reakcie na incidenty</li> </ul>	X	✓