ESET aktualizuje platformu ESET PROTECT, nová funkce pomůže s obnovou po útoku ransomwarem

26.3.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET, přední světový poskytovatel řešení v oblasti kybernetické bezpečnosti, aktualizovala svou platformu ESET PROTECT, která je součástí nabídky pro zákazníky z řad firem, organizací a institucí. Aktualizovaná nabídka nově obsahuje funkci Obnova po útoku ransomwarem. ESET tak svým zákazníkům poskytne nový způsob řešení této globální kybernetické hrozby. Mimo to aktualizace obsahuje také nové funkcionality pro řešení ESET Cloud Office Security s cílem posílit zabezpečení e-mailové komunikace – ochranu proti spoofingu (technika, při které se útočníci vydávají za jinou osobu nebo zařízení) a před útoky využívajícími tzv. homoglyfy (znaky, které pochází z jiných abeced, ale jsou zaměnitelné s latinským písmem). Aktualizace přináší vylepšení stability a výkonu také pro AI asistenta ESET AI Advisor.

„Společnost ESET má bohatou historii s bojem proti ransomwaru. Týká se to nejen naší platformy pro zabezpečení koncových zařízení či našich služeb, jako je ESET MDR, ale i naší účasti v iniciativě No More Ransom. S funkcí Obnova po útoku ransomwarem bychom chtěli zdůraznit, že k ochraně před sofistikovanými ransomwarovými útoky firmy nepotřebují celou armádu zaměstnanců. Stačí jednoduché řešení a pár kliknutí — zbytek nechte na ESET," říká Michal Jankech, viceprezident pro segment Enterprise & SMB/MSP ve společnosti ESET.

Před touto aktualizací pracovala vícevrstvá technologie ESET LiveSense na proaktivní prevenci před ransomwarem a dalšími sofistikovanými útoky prostřednictvím funkcionalit Ochrana proti ransomware, Ochrana proti síťovým útokům či Host-Based Intrusion Prevention System (HIPS). Konkrétně funkcionalita Ochrana proti ransomware, která monitoruje a vyhodnocuje všechny spuštěné aplikace na základě jejich chování a reputace, je navržena tak, aby detekovala a blokovala procesy, které se podobají chování ransomwaru. Novou aktualizací se inciativa přesouvá od útočníků do rukou samotných firem. ESET vylepšuje ochranu o funkci Obnova po útoku ransomwarem, vlastní řešení zálohování, které je vytvořené k ochraně proti zašifrování.

„Útoky ransomwarem se stávají stále sofistikovanějšími. Útočníci se snaží narušit každý aspekt bezpečnostní stability, kterou firma má. Klíčovým prvkem těchto útoků je zašifrování, které zablokuje firmě přístup k jejím podnikovým systémům, naruší její procesy s významnými dopady do jejích nákladů, a nakonec ji nutí zaplatit za dešifrování jejích systémů. V loňském roce útočníci dokonce poprvé požadovali za zpřístupnění dat rekordní částku 100 milionů dolarů. Útočníci jdou tak daleko, že cílí i na zálohy systémů, které mažou nebo poškozují. Běžnou součástí útoků ransomwarem jsou i škodlivé kódy, které se snaží vypnout bezpečnostní řešení. Nenechávají nic náhodě. Obnova je pak často nemožná a náklady na odstranění následků útoku se zvyšují. S tím, jaký vývoj v případě ransomwaru sledujeme, je tak stále reálnější hrozbou pro firmy a organizace bez ohledu na jejich velikost. Alarmujícím trendem roku 2024 byl například celosvětový rapidní růst útoků na sektor zdravotnictví a je bohužel možné, že tento trend bude pokračovat i letos," říká Jakub Souček, vedoucí pražského výzkumného týmu společnosti ESET.

Funkce Obnova po útoku ransomwarem funguje ve spolupráci se stávající technologií Ochrana proti ransomware. Ta novou funkci instruuje k vytvoření záloh, jakmile detekuje podezřelou aktivitu. Funkce bude takto pracovat až do té doby, dokud Ochrana proti ransomware nerozhodne, že proces

je v pořádku. V tom okamžiku je zálohování zrušeno. Pokud se jedná o škodlivý proces, funkce činnost ransomwaru ukončí a obnoví soubory ze zálohy.

„Na rozdíl od jiných řešení, která jsou založena na službě Windows Volume Shadow Copy, nemohou být zálohy, které nová funkce Obnova po útoku ransomwarem vytvoří, zneužity útočníky. Funkce má vlastní chráněné úložiště, kde útočníci nemohou soubory modifikovat, poškodit ani smazat. Tím se aktivně řeší jeden z nejčastějších nedostatků běžných záloh během útoku ransomwarem," vysvětluje Martin Skýpala, produktový specialista z pražské pobočky společnosti ESET.

Jediným skutečným omezením funkce je velikost disku a limit velikosti jednoho souboru do 30 MB. Administrátoři, kteří s platformou ESET PROTECT pracují, by proto měli určit, které typy souborů přidat do filtru funkce, aby je zahrnula během své činnosti do vytvoření zálohy.

Funkce Obnova po útoku ransomwarem je zahrnuta jako bezplatný doplněk v řešení ESET PROTECT Advanced a vyšších řešeních. Je dostupná pouze pro systémy založené na operačním systému Windows. Ke správnému fungování této funkce je nezbytné, aby byla povolena Ochrana proti ransomware. Zákazníci jsou nicméně chráněni od samého začátku, protože ochrana je aktivována už ve výchozím nastavení.

Kromě výše zmíněné funkce je součástí aktualizace také nová ochrana proti spoofingu a útokům využívajícím homoglyfy. Nově je součástí stávajícího řešení ESET Cloud Office Security (ECOS). Útočníkům brání v tom, aby se vydávali za důvěryhodné zdroje či osoby a rozpozná, pokud chtějí maskovat škodlivé domény nebo URL adresy záměnou písmen z jiných abeced. ESET Cloud Office Security navíc nyní také obsahuje funkci zpětného stažení e-mailů, která umožňuje rychle odvolat a umístit do karantény jakékoli doručené e-maily, které vyhodnotí jako podezřelé. To vše je možné sledovat v rámci nových dashboardů, které nabízejí plně přizpůsobitelné záložky a komponenty. Díky vizuálnímu vylepšení a novým prvkům tak odpovídají specifickým potřebám uživatelů a uživatelek.

ESET AI Advisor prošel dále vylepšením stability a výkonu a nyní může pracovat s incidenty, které jsou automaticky vytvořeny prostřednictvím řešení ESET Inspect nebo které se generují v rámci služby Spravované detekce a reakce (MDR). S větším množstvím dat ke zpracování může ESET AI Advisor nabídnout ještě lepší poradenství SOC týmům a poskytnout bezpečnostním analytikům vylepšení pracovních postupů. ESET AI Advisor je nyní také dostupný jako doplněk k úrovním ESET PROTECT Enterprise, ESET PROTECT Elite a ESET PROTECT MDR. Zdarma je potom součástí ESET PROTECT MDR Ultimate.

Více informací o platformě ESET PROTECT najdete na našich webových stránkách. Více informací o útocích a o aktuálním dění na ransomwarové scéně můžete najít mezi našimi tiskovými zprávami anebo na stránkách magazínu o kybernetické bezpečnosti pro firmy Digital Security Guide.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-aktualizuje-platformu-eset-protect-no

va-funkce-pomuze-s-obnovou-po-utoku-ransomwarem