ESET odhalil nové vazby mezi konkurenčními ransomwarovými gangy, snaží se vypnout obranné technologie

31.3.2025 - | ESET software

Praha, 31. března 2025 – Bezpečnostní experti ze společnosti ESET vydali novou, podrobnou analýzu o významných změnách v ekosystému ransomwarových gangů. Analýza se zaměřuje na nově vzniklý a aktuálně dominantní gang RansomHub, který funguje v modelu ransomware-as-a-service (RaaS). Experti v nové analýze sdílí zatím nepublikované informace o organizační struktuře partnerů tohoto gangu. Odkrývají také dosud nezdokumentované spojení mezi tímto gangem a dalšími, již zavedenými ransomwarovými skupinami Play, Medusa a BianLian. Analýza dále nabízí nový pohled na škodlivý kód EDRKillShifter. Jedná se o vlastní nástroj útočníků určený k vypnutí EDR (Detekce a reakce na hrozby pro koncová zařízení). Jak experti zdůrazňují, hrozby v podobě těchto nástrojů jsou v současnosti na vzestupu.

„V celosvětovém boji proti ransomwaru jsme mohli v roce 2024 sledovat dosažení dvou milníků: Dva dříve největší ransomwarové gangy, LockBit a BlackCat, zmizely ze scény. A poprvé od roku 2022 jsme zaznamenali, že finanční náklady spojené s útoky ransomwarem výrazně klesly, a to o 35 procent, což je v tomto kontextu ohromující číslo. Na druhou stranu ale podle webových stránek, které veřejně publikují informace o útocích a únicích dat, vzrostl zaznamenaný počet obětí přibližně o 15 procent. Velkou část tohoto nárůstu má na svědomí právě RansomHub, nový gang fungující v modelu ransomware-as-a-service. Jedná se o model fungování útočníků v ekosystému operátorů (autorů) ransomwaru, partnerů, kteří si škodlivý kód pronajímají a útočí na vybrané cíle, a tzv. infiltrátorů, kteří zajistí partnerům přístup k lukrativním cílům," říká Jakub Souček, vedoucí pražského výzkumného týmu společnosti ESET.

„Gang RansomHub se objevil přibližně ve stejné době, kdy se orgánům činným v trestním řízení podařilo v mezinárodní operaci Cronos narušit aktivity gangu LockBit. Dynamicky se proměňující ransomwarové prostředí samozřejmě není dobrou zprávou pro firmy a instituce, které se této neustále přítomné hrozbě musí přizpůsobovat, zvlášť pokud spadají do oblasti kritické infrastruktury. Reakci lze vidět i v legislativní oblasti, kde v České republice na boj s touto hrozbou klade důraz například i nový Zákon o kybernetické bezpečnosti," dodává Souček.

Stejně jako jakýkoli jiný vznikající gang, i RansomHub potřeboval přilákat partnery, kteří si pronajmou služby ransomwaru od jeho operátorů. Počáteční inzerát útočníci zveřejnili na rusky mluvícím fóru RAMP začátkem února 2024, osm dní před zveřejněním prvních obětí. Gang RansomHub zakazuje provádět útoky na země postsovětského Společenství nezávislých států, Kubu, Severní Koreu nebo Čínu. Zajímavostí je také to, že gang láká partnery s příslibem, že si mohou ponechat ve svých peněženkách většinu platby (až 90 %) za výkupné od napadených obětí. O zbylých 10 procent z výkupného se pak musí partneři podělit s operátory. Právě důvěra operátorů v partnery, že jim tuto částku skutečně pošlou, je v prostředí ransomwarových gangů unikátní.

V květnu 2024 pak operátoři gangu RansomHub významným způsobem aktualizovali podobu útoku: přidali svůj vlastní nástroj k vypnutí technologie EDR. Cílem tohoto speciálního typu škodlivého kódu je ukončit, zmást nebo obejít bezpečností software, který má oběť nainstalovaný ve svém systému. Dochází k tomu obvykle prostřednictvím zranitelného ovladače.

Nástroj k zneškodnění EDR s názvem EDRKillShifter gang RansomHub sám vyvinul, spravuje ho a nabízí k použití svým partnerům. Funkčně se jedná o typickou technologii ke zneškodnění EDR v rámci široké škály různých bezpečnostních řešení, na které útočníci předpokládají, že narazí při pokusu o proniknutí do sítí svých obětí.

„Rozhodnutí implementovat takovou technologii a nabídnout ji partnerům jako součást programu RaaS je vzácné. Partneři musí obvykle sami najít způsoby, jak bezpečnostní řešení obejít. Někteří používají již existující nástroje, zatímco více technicky zaměření útočníci si takové nástroje dále upravují pro vlastní potřeby. Někteří mohou využít i nástroje, které jsou jako služby dostupné na dark webu. Zaznamenali jsme prudký nárůst využívání nástroje EDRKillShifter, a to nejen v případě útoků gangu RansomHub," vysvětluje Souček z ESETu.

Bezpečnostní experti z ESETu zjistili, že partneři gangu RansomHub pracují pro tři další soupeřící gangy — Play, Medusa a BianLian. Odhalení spojení mezi gangy RansomHub a Medusa není překvapivé, protože je obecně známo, že partneři z ransomwarového prostředí často pracují pro více operátorů současně. Na druhou stranu je ale nepravděpodobné, že by si gangy Play a BianLian najaly stejného partnera gangu RansomHub, a to kvůli uzavřené povaze těchto skupin útočníků. Je to ale jedno z možných vysvětlení, proč mají gangy Play a BianLian přístup ke škodlivému kódu EDRKillShifter. Daleko pravděpodobnější je nicméně scénář, ve kterém důvěryhodní členové gangů Play a BianLian spolupracují s rivaly, dokonce i s nově vzniklými jako RansomHub, a pak používají jejich nástroje pro své vlastní útoky. Ransomwarový gang Play je také spojován se skupinou Andariel, která je napojena na Severní Koreu.

Více informací a technických podrobností o gangu RansomHub a technologii EDRKillShifter najdete v článku na webu welivesecurity.com.

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.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561

vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-odhalil-nove-vazby-mezi-konkurencnimi-ransomwarovymi-gangy-snazi-se-vypnout-obranne-technologie