# ESET zmapoval nejnovější aktivity ransomwarového gangu CosmicBeetle, který útočil na organizace a firmy v Česku

**16.9.2024 - Lucie Mudráková | ESET software**

**Bezpečnostní analytici společnosti ESET popsali chování nového ransomwaru ScRansom, který pro své útoky vyvinula skupina CosmicBeetle. Cílem tohoto ransomwarového gangu jsou především malé a střední firmy v Asii a v Evropě, včetně České republiky.**

**Své oběti napadá prostřednictvím několik let starých zranitelností v jejich systémech. Podle zjištění společnosti ESET skupina experimentuje s uniklým nástroji nechvalně proslulé kyberkriminální skupiny LockBit a využívá její známé jméno k tomu, aby útoky vypadaly přesvědčivěji a přiměla oběti zaplatit výkupné. Podle expertů je také možné, že se skupina CosmicBeetle stala v nedávné době partnerem ransomwarového gangu RansomHub, který na ransomwarové scéně působí od března 2024 a patří k nejaktivnějším útočníkům současnosti. Bezpečnostní experti před útoky gangu CosmicBeetle varují, protože jeho nespolehlivé procesy zašifrování a dešifrování nemusí vždy vést k úspěšné obnově souborů po útoku**.

Bezpečnostní experti z ESETu popsali v nové analýze nedávné aktivity ransomwarového gangu CosmicBeetle, zdokumentovali nasazení jeho nového ransomwaru ScRansom a objevili jeho propojení s dalšími dlouhodobě aktivními ransomwarovými gangy. Skupina CosmicBeetle cílí na malé a střední firmy (SMBs) v Asii a v Evropě. Stopy útoků vedou i do České republiky, kde mezi jejími oběťmi byly například firmy z oblasti výroby nebo územní orgány státní správy.

„Ransomware je jednou z největších crimeware hrozeb nejen ve světě, ale i v Česku, kde jsou dlouhodobě nejohroženějšími oblastmi zdravotnictví, školství a veřejná správa. Cílem těchto útoků je již tradičně finanční zisk. Z povahy věci tak velké a sofistikované gangy útočí především na velké organizace, malé a střední podniky jsou naopak zajímavými cíli pro menší a méně zkušené gangy. Tyto organizace a firmy totiž většinou nedisponují robustní ochranou a procesy pravidelných bezpečnostních aktualizací, které by je mohly před těmito útoky účinně ochránit," říká Jakub Souček, bezpečnostní expert z pražské výzkumné pobočky společnosti ESET, který stojí v čele týmu zabývajícím se mezinárodní kyberkriminalitou.

„Podle našich pravidelných průzkumů patří únik nebo krádež dat mezi hrozby, kterých se firmy v Česku obávají nejvíce – s pokusem o útok ransomwarem se každý měsíc setká až desítka z nich. V případě gangu CosmicBeetle by pak firmy a organizace určitě neměly podcenit adekvátní ochranu před ransomwarem. Jelikož se jedná o mladého aktéra, který své škodlivé kódy a nástroje neustále vyvíjí, nedá se spolehnout na to, že budou vždy správně fungovat. Obnova dat pak nemusí být ani při zaplacení zaručena a nejlepší obranou je tak prevence," dodává Souček.

Podle společnosti ESET skupina využívá zveřejněný builder nechvalně proslulého ransomwarového gangu LockBit, který je v současnosti ve své aktivitě oslabený díky operaci Cronos z února 2024. Podle bezpečnostních specialistů se skupina CosmicBeetle snaží „přiživit" na reputaci tohoto aktéra a využít jeho značku ve svých útocích. Kromě těchto zjištění je také pravděpodobné, že CosmicBeetle je novým partnerem gangu RansomHub, který funguje jako tzv. rasnomware-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. RansomHub je aktivní od letošního března a velmi rychle se vyšplhal mezi nejvýraznější aktéry na mezinárodní ransomwarové scéně.

„Napsat od nuly vlastní ransomwarový kód může přinášet řadu překážek. Pravděpodobně i z toho důvodu se skupina CosmicBeetle rozhodla, že využije reputaci gangu LockBit. Může za tím být snaha zakrýt nějaké problémy v základním kódu a zvýšit tak šanci, že oběti přesto zaplatí," vysvětluje Souček. „Nedávno jsme navíc také zpozorovali nasazení dvou různých ransomware vzorků na stejném zařízení, a to s odstupem jen jednoho týdne. Jednalo se o ransomware ScRansom a ransomware, který typicky využívá gang RansomHub. To bylo v porovnání s běžnými incidenty skupiny RansomHub, které v naší telemetrii vídáme, velmi neobvyklé. Zároveň jsme však našli několik shodných charakteristik s chováním skupiny CosmicBeetle. Vzhledem k tomu, že v případě gangu RansomHub nejsou evidovány žádné úniky jeho kódů na veřejnost, je zde určitá možnost, že skupina CosmicBeetle byla v nedávné době partnerem gangu RansomHub," dodává Souček.

Skupina CosmicBeetle často používá tzv. útoky hrubou silou k prolomení obrany systémů svých obětí. Kromě toho zneužívá také řadu známých zranitelností. Mezi její nejčastější oběti patří malé a střední podniky z různých odvětví po celém světě. Segment malých a středních firem obvykle využívá softwarové nástroje, které jsou těmito útoky postiženy. Tyto organizace také často nemají zavedené robustní procesy správy bezpečnostních záplat. ESET zaznamenal útoky v následujících odvětvích a oblastech: výroba, farmacie, právní služby, vzdělávání, zdravotnictví, technologie, pohostinství, finanční služby či územní orgány státní správy.

Kromě zašifrování souborů může ransomware ScRansom zastavit také různé procesy a služby na postiženém zařízení. ScRansom není příliš pokročilý ransomware, přesto se skupině CosmicBeetle podařilo napadnout významné cíle a způsobit jim velké škody. Oběti postižené ransomwarem ScRansom by tak měly být opatrné, pokud se rozhodnou útočníkům za dešifrování souborů zaplatit. CosmicBeetle je totiž stále nezkušený ransomwarový gang a nasazení škodlivého kódu ScRansom provází problémy.

Bezpečnostním expertům z ESETu se podařilo získat dešifrovací nástroj skupiny CosmicBeetle, který využívala ve svých nedávných útocích. Škodlivý kód ScRansom prochází neustálým vývojem, což není z hlediska ransomwarových útoků nikdy dobré znamení – přílišná komplikovanost procesu zašifrování (a dešifrování) vytváří prostor pro chyby, což má vliv na to, jak úspěšné bude obnovení všech souborů. Úspěšné dešifrování závisí na správné funkci dešifrovacího nástroje a na tom, zda útočníci z CosmicBeetle poskytnou všechny potřebné dešifrovací klíče.

Skupina CosmicBeetle je aktivní minimálně od roku 2020 a název ji experti z ESETu přiřadili po jejím objevení v roce 2023. Tento ransomwarový gang je nejvíce známý používáním své vlastní sbírky nástrojů psaných v jazyce Delphi, souhrnně nazývaných Spacecolon.

Podrobné technické informace o útocích ransomwarového gangu CosmicBeetle najdete na webu welivesecurity.com.

Týmy bezpečnostních expertů společnosti ESET pravidelně představují závěry svých analýz prostřednictvím tiskových zpráv a odborných publikací, či na řadě významných konferencí, jako je například Virus Bulletin, Botconf nebo Prague Cyber Security Conference. Mezi poslední úspěšné akce patří kromě loňského rozkrytí fungování organizovaných skupin na internetových bazarech například také spolupráce na rozbití botnetu Grandoreiro ve spolupráci s brazilskou federální policií.

Více informací o trendech v kyberbezpečnosti najdete například v online magazínu o IT bezpečnosti pro firmy Digital Security Guide.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-zmapoval-nejnovejsi-aktivity-ransomwaroveho-gangu-cosmicbeetle-ktery-utocil-na-organizace-a-firmy-v-cesku