ESET přináší závěry z vyšetřování ransomwarového gangu Gentlemen, který operuje také v České republice

18.6.2026 - | ESET software spol. s r.o. - Eset.com

Bezpečnostní experti ze společnosti ESET analyzovali robustní sadu nástrojů pro obcházení zabezpečení, tzv. EDR killery, které využívá ransomwarový gang Gentlemen. Skupina funguje jako RaaS (ransomware-as-a-service), což je 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. Od začátku roku 2026 se útočníci z gangu Gentlemen zařadili mezi nejaktivnější skupiny v tomto ekosystému. Skupina se od ostatních odlišuje pokročilou sadou nástrojů pro obcházení detekce a reakce na koncových zařízeních (EDR). Na rozdíl od většiny dalších předních gangů se Gentlemen nezaměřuje primárně na oběti v USA. Mimo Thajsko, Brazílii či Francii útočníci operují také například v České republice.

„V posledních měsících se objevovalo několik různých analýz ransomwarového gangu Gentlemen, nezaměřovaly se nicméně na detailní popis jeho nástrojů pro vypínání EDR. ESET má kontinuální vhled do incidentů spojovaných s tímto gangem, a může tak poskytnout jedinečný a komplexní obraz o tom, jak skupina EDR killery vyvíjí a používá. Gang navíc v květnu letošního roku zasáhl únik interních dat, díky kterému jsme získali další cenné informace o jeho fungování," říká Jakub Souček, vedoucí výzkumného týmu v pražské pobočce společnosti ESET, který se specializuje na monitorování mezinárodní kyberkriminality.

„V únoru 2026 jsme detekovali poměrně unikátní sadu nástrojů k vypínání zabezpečení v rukou gangu Gentlemen. Už tehdy jsme s vysokou pravděpodobností předpokládali, že nástroje jsou spravovány a z velké části také vyvíjeny přímo vedením gangu. Nedávno uniklá data nám tuto hypotézu definitivně potvrdila. Sadu nástrojů, které gang sám vyvíjí, jsme souhrnně označili jako GentleKiller," dodává Souček.

Ransomwarový gang Gentlemen se objevil na konci roku 2025. Rychle se vypracoval mezi nejaktivnější ransomwarové skupiny pozorované během prvního čtvrtletí roku 2026. Skupina nabízí svým partnerům velkorysý podíl ve výši 90 % zisků z operací. Gentlemen své oběti vydírá dvojím způsobem — kromě šifrování dat také vyhrožuje jejich zveřejněním, pokud oběť nezaplatí výkupné.

Útočníci ze skupiny Gentlemen se od ostatních velkých hráčů odlišují. Jednou z těchto odlišností je jejich ochota poskytnout svým partnerům několik nástrojů k různým účelům – kromě nástroje pro šifrování také nástroje k obcházení EDR. Výběr cílů většinou zajišťují partneři gangů, přičemž u ostatních velkých ransomwarových gangů převažuje jeden vzorec, a to výrazné a dlouhodobé zacílení na oběti v USA. Tyto oběti často tvoří přibližně polovinu všech zveřejněných obětí útoků ransomwarem. Gentlemen jsou opět výraznou výjimkou. Ačkoli se za první čtvrtletí letošního roku řadí mezi pět nejaktivnějších ransomwarových skupin, cílí konzistentně na oběti napříč širokým a geograficky různorodým spektrem zemí. Významná část obětí pochází z regionů, jako jsou jihovýchodní Asie, Jižní Amerika a západní Evropa, podle informací bezpečnostních expertů ale gang operuje také v Česku.

„Jak jsme již informovali na jaře letošního roku, Gentlemen je jedním z gangů, které se cíleně zaměřují i na subjekty v České republice. Ransomwarové gangy se v Česku zaměřují především na

malé a středně velké firmy, SMB. Tento segment je pro útočníky lákavý, protože tyto firmy mají zpravidla omezené kapacity v oblasti kybernetické bezpečnosti, dopady výpadku systémů jsou pro provoz závažnější a pravděpodobnost zaplacení výkupného je vyšší. Aktuálně je na veřejných stránkách ransomwarových skupin evidováno již 20 českých obětí od začátku roku 2026, přičemž za celý minulý rok jich bylo 22. Převažují u nás oběti z oblasti výroby, technologického sektoru a obchodu," doplňuje Souček.

Skupina dále také využívá nástroje, které jí poskytují třetí strany nebo uniknou na dark web. Jde například o nástroje, které ESET označuje jako HexKiller, ThrottleBlood a HavocKiller. Všechny EDR killery skupiny Gentlemen, ať už vyvinuté či získané odjinud, spojuje společná strategie, jak uniknout pozornosti obránců. Útočníci je vydávají převážně za legitimní bezpečnostní software pomocí falešných informací, jako jsou verze programu či kopie certifikátů a ikon. Útočníci z gangu Gentlemen zároveň dokážou neobvykle rychle uvést do praxe postupy, které bývají do té doby jen tzv. proof of concept, a to v řádech několika dní od jejich zveřejnění. Často se jedná o scénáře typu Bring Your Own Vulnerable Driver, útok pomocí zranitelného či škodlivého ovladače. Kromě nástrojů, které vypínají EDR, experti identifikovali také nástroj určený ke krádeži přihlašovacích údajů, který nazvali OxideHarvest, a za jehož vývojem stojí jeden z partnerů gangu Gentlemen.

Bezpečnostní experti z ESETu doposud identifikovali osm odlišných variant systému GentleKiller, z nichž každá se vydává za jiný legitimní program a zneužívá odlišný zranitelný nebo škodlivý ovladač. Navzdory těmto rozdílům však ESET všechny tyto vzorky klasifikuje pod označením GentleKiller, a to kvůli vysokému počtu sdílených interních znaků.

„Z pohledu obrany nám pochopení toho, jak funguje GentleKiller, umožňuje lépe navrhnout naše obranné strategie a bránit se i proti dosud nevyvinutým nástrojům v arzenálu gangu Gentlemen," uzavírá Souček z ESETu.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

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

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

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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-prinasi-zavery-z-vysetrovani-ransomwaroveho-gangu-gentlemen-ktery-operuje-take-v-ceske-republice