ESET popsal kyberšpionáž Ruskem podporované skupiny Gamaredon, cílem byla Ukrajina a země NATO

4.10.2024 - Lucie Mudráková | ESET software

Bezpečnostní analytici společnosti ESET prozkoumali kyberšpionážní operace APT skupiny Gamaredon napojené na Rusko. Gamaredon je v současnosti nejaktivnější APT skupinou na Ukrajině a většina jejích kyberšpionážních útoků je vedena proti ukrajinským vládním institucím. ESET ale zaznamenal také několik pokusů o napadení cílů v zemích NATO – konkrétně v Bulharsku, Lotyšsku, Litvě a Polsku.

Ani v jednom z těchto případů však útok nebyl úspěšný. Skupina Gamaredon v poslední době výrazně vylepšila své schopnosti v provádění kyberšpionáže a vyvinula několik nových nástrojů pro krádež cenných dat z aplikací poskytovatelů e-mailových služeb, chatovacích aplikací jako je Signal nebo Telegram a webových aplikací. Analýza expertů z ESETu odhalila také infostealer PteroBleed, který skupina využívá k odcizení dat z ukrajinského vojenského systému.

APT skupina Gamaredon je aktivní minimálně od roku 2013 a v současnosti patří k nejaktivnějším útočníkům na Ukrajině. APT (Advanced Persistent Threat) je označení pro uskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby a obvykle mají podporu států.

Skupina Gamaredon je na základě informací Služby bezpečnosti Ukrajiny (SSU) spojována s ruským 18. centrem informační bezpečnosti FSB, které operuje z okupovaného Krymu. Bezpečnostní experti společnosti ESET jsou přesvědčeni, že tato skupina úzce spolupracuje s další skupinou útočníků, kterou objevili a pojmenovali InvisiMole. Většina kyberšpionážních útoků skupiny Gamaredon je vedena proti vládním institucím na Ukrajině. V dubnu 2022 a únoru 2023 však ESET zaznamenal také několik pokusů o napadení cílů v několika zemích NATO, jmenovitě v Bulharsku, Lotyšsku, Litvě a Polsku. Žádný z těchto pokusů však nebyl úspěšný.

„APT skupinu Gamaredon sledujeme dlouhodobě. Jedná se o útočníky, kteří nevyužívají sofistikované nástroje, byť patří mezi státem podporované skupiny, které k tomu mají finanční prostředky. Spolupracují s další APT skupinou InvisiMole, která za ně tento nedostatek kompenzuje. Skupina Gamaredon se historicky specializovala především na Ukrajinu a rozšíření jejích aktivit na státy NATO není typické. Na druhou stranu a s ohledem na polohu těchto zemí je jejich zájem o tento region v konečném důsledku očekávaný. I přestože v tuto chvíli nevidíme žádný útok zacílený na Českou republiku, nelze ho do budoucna vyloučit," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET.

Skupina Gamaredon využívá různé techniky tzv. obfuskace (úpravy zdrojového kódu s cílem znemožnit jeho analýzu) a řadu metod k obcházení blokování na úrovni domén. Tyto taktiky kladou velké výzvy snahám sledovat aktivity útočníků, protože ztěžují automatickou detekci a blokování jejich nástrojů. Během vyšetřování se nicméně expertům z ESETu podařilo tyto taktiky identifikovat a pochopit, a pokračovat tak ve sledování aktivit této APT skupiny. Skupina Gamaredon používá vlastní škodlivé nástroje proti svým cílům systematicky a začala s tím již dlouho před začátkem ruské invaze v roce 2022. K napadení nových obětí využívá spearphishingové kampaně a také vlastní malware. Jeho prostřednictvím útočníci nakazí dokumenty programu Word či USB disky, ke kterým mají přístup počáteční oběti útoků. Útočníci pak očekávají, že je budou sdílet s dalšími uživateli a

dojde tak k rozšíření malwaru k dalším potenciálním obětem.

Během roku 2023 skupina výrazně zlepšila své schopnosti k uskutečnění kyberšpionáže a vyvinula několik nových nástrojů ve skriptovacím jazyce PowerShell. Tyto nástroje pak slouží ke krádeži dat z e-mailových klientů, chatovacích aplikací, jako je Signal nebo Telegram, a webových aplikací běžících v internetových prohlížečích. Ke krádeži dat skupina využívá také infostealer PteroBleed, který experti z ESETu objevili v srpnu 2023. Infostealer je určený ke krádeži dat z ukrajinského vojenského systému a z webmailové služby používané ukrajinskou vládní institucí.

„Útočníci ze skupiny Gamaredon se na rozdíl od většiny APT skupin nesnaží být nenápadní a zůstat při kyberšpionáži co nejdéle skrytí díky využívání nových technik. Operátoři z této skupiny jsou spíše bezohlední a nevadí jim, že je obránci systémů během jejich aktivit objeví. Přesto ale vynakládají velké úsilí na to, aby se vyhnuli blokování bezpečnostními řešeními a velmi se snaží udržet si přístup ke kompromitovaným systémům," vysvětluje Šuman.

„Typicky si skupina snaží zachovat svůj přístup k napadeným systémům tím, že do útoků zapojí současně několik jednoduchých downloaderů nebo backdoorů – tzv. zadních vrátek. Nedostatek sofistikovaných nástrojů také kompenzuje častými aktualizacemi a využíváním rychle se měnící obfuskace. Navzdory tomu, že tyto nástroje jsou relativně jednoduché, obávanou hrozbu činí ze skupiny hlavně její vytrvalost a agresivní přístup. Vzhledem k probíhající válce na Ukrajině očekáváme, že se skupina Gamaredon bude na tento region zaměřovat i nadále," uzavírá Šuman z ESETu.

Podrobné technické informace o kyberšpionážních útocích APT skupiny Gamaredon najdete na webu welivesecurity.com a v díle podcastu TruePositive, který byl věnován APT skupinám napojeným na Rusko.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

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-popsal-kyberspionaz-ruskem-podporovane-skupiny-gamaredon-cilem-byla-ukrajina-a-zeme-nato