ESET vydal zprávu o aktivitách státy podporovaných útočníků, nejvíce operací bylo spojeno s Ruskem

20.5.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Nejnovější zpráva společnosti ESET, APT Activity Report, shrnuje zásadní aktivity útočných skupin, které byly sledovány bezpečnostními experty společnosti od října 2023 do konce března 2024.

Hlavními cíli většiny útočných kampaní byly vládní organizace. Skupiny napojené na Rusko se zaměřily na špionáž v rámci Evropské unie a pokračovaly také v útocích proti Ukrajině. Za největším počtem sledovaných operací stáli dle zprávy právě především kyberútočníci napojení na Rusko. Bezpečnostní experti sledovali také další vývoj operace Texonto, v jejímž rámci útočníci šíří prostřednictvím e-mailového spamu dezinformace s cílem znejistit ukrajinské obyvatelstvo doma i v zahraničí. Útočné skupiny napojené na Írán zvýšily také svou aktivitu, a to především proti Izraeli po útoku vedeném hnutím Hamás v říjnu 2023 a během probíhající války v Gaze. Skupiny spojené s Čínou pak zneužívaly zranitelnosti veřejně přístupných zařízení a softwaru.

ESET vydal svou nejnovější zprávu APT Activity Report, která je souhrnem aktivit vybraných útočných APT skupin. APT (Advanced Persistent Threat) je označení pro uskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby a obvykle mají podporu států. Aktuální report je souhrnem analýz společnosti ESET od října 2023 do konce března 2024.

Vybrané útočné kampaně, kterým je aktuální zpráva věnována, pokrývají širší oblast kybernetických hrozeb a jsou v souladu s aktuálními klíčovými trendy a vývojem této oblasti. APT skupiny podporované Ruskem se ve sledovaném období zaměřily na špionáž v rámci Evropské unie a nadále útočily také na Ukrajinu. APT skupiny spojené s Íránem zintenzivnily svou aktivitu po útoku hnutí Hamás na Izrael v říjnu 2023 a v kontextu probíhající války v Gaze. Skupiny podporované Čínou zneužívaly zranitelnosti veřejně přístupných zařízení, jako jsou VPN a firewally, a softwaru, například služeb Confluence a Microsoft Exchange Server, pro počáteční přístup ke svým obětem napříč různými odvětvími. Skupiny spojené se Severní Koreou nadále cílily především na letecký a obranný průmysl a na odvětví kryptoměn.

„Cílem většiny kampaní, kterým se věnujeme v aktuální zprávě, byly vládní organizace a některá konkrétní odvětví, například ta spojená s pokračujícími a neúnavnými útoky na ukrajinskou infrastrukturu. Evropa zažila ve sledovaném období pestrou škálu útoků od různých kyberútočníků," říká Robert Šuman, vedoucí výzkumné pobočky společnosti ESET v Praze. „Skupiny spojené s Ruskem posílily své špionážní aktivity v Evropské unii, kde jsou stále přítomni také útočníci napojení na Čínu – to naznačuje trvalý zájem těchto APT skupin o dění v evropském prostoru," dodává Šuman.

Mezi aktivitami útočných skupin spojených s Ruskem zjistili bezpečnostní experti další informace k PSYOP operaci Texonto. V jejím rámci se šířily další dezinformace kolem protestů souvisejících s ruskými volbami a situace ve východoukrajinském městě Charkov, což utvrzuje nejistotu mezi Ukrajinci doma i v zahraničí.

„Za sledované období jsme viděli, že nejvíce útoků pocházelo od skupin, které jsou napojeny na Rusko. Jejich cílem je především Ukrajina, kde nejvíce operují dvě nechvalně proslulé APT skupiny –

Gamaredon, která je aktuálně na Ukrajině nejvíce aktivní, a Sandworm, která dlouhodobě cílí především na ukrajinskou energetickou infrastrukturu," říká Šuman. „Na Ukrajině jsme především v prvních měsících války pozorovali využívání destruktivního malwaru typu wiper, jehož úkolem je ničit data, zatímco v posledních měsících vzrostly především kyberšpionážní operace. PSYOP operace Texonto nám nyní ukazuje další rozměr války v kyberprostoru – cílené šíření dezinformací prostřednictvím spamové kampaně, které mají za úkol znejistit obyvatelstvo a zasévat do společnosti rozpory," dodává Šuman.

Ruskem podporované skupiny využívají převážně spearphishingové e-maily k získání počátečního přístupu do sítí svých obětí. V jedné kampani, kterou bezpečnostní experti analyzovali, obsahovaly e-maily buď nebezpečné odkazy, nebo přílohy. Pokud na ně oběti klikly nebo přílohy otevřely, malware se zaměřil na získání přihlašovacích údajů nebo přímo na instalaci škodlivých kódů do jejich systémů. Od konce února 2024 pozoroval ESET vlnu spearphishingových e-mailů zaměřených na evropské vládní instituce. Jejich prostřednictvím se útočníci snažili využít zranitelnost CVE-2024-21413 v aplikaci Outlook, známou také jako bezpečnostní chybu Moniker Link.

Na základě úniku dat z čínské společnosti I-SOON (Anxun), která nabízí bezpečnostní služby, může ESET potvrdit, že se tato čínská společnost ve skutečnosti zabývá kyberšpionáží. ESET sleduje část aktivit této firmy také pod činností APT skupiny FishMonger. V nejnovější zprávě ESET představuje také novou APT skupinu navázanou na Čínu, CeranaKeeper, která i přesto, že má své vlastní svébytné znaky, je možná spojena s digitálním otiskem APT skupiny Mustang Panda.

Pokud jde o útočníky podporované Íránem, skupiny MuddyWater a Agrius změnily své předchozí zaměření na kyberšpionáž a ransomware směrem k agresivnějším strategiím, které zahrnují například zprostředkování přístupu a útoky s dopadem (např. pomocí wiperů). Intenzita aktivit skupin OilRig a Ballistic Bobcat naopak poklesla, což naznačuje strategický posun směrem k nápadnějším a „hlasitějším" operacím zaměřeným na Izrael.

Zpráva také popisuje zneužití zero-day zranitelnosti v aplikaci Roundcube skupinou Winter Vivern, která je dle dat společnosti ESET pravděpodobně spojena s Běloruskem. Společnost ESET také ve zprávě upozorňuje na kampaň probíhající na Středním východě pod vedením skupiny SturgeonPhisher, která pravděpodobně sleduje zájmy Kazachstánu.

Bezpečnostní řešení společnosti ESET chrání systémy našich zákazníků před škodlivými aktivitami popsanými v této zprávě. Informace zde sdílené jsou převážně založeny na vlastních unikátních telemetrických datech společnosti ESET a byly ověřeny výzkumnými analytiky společnosti, kteří připravují podrobné technické zprávy a pravidelné aktuality o činnostech konkrétních APT skupin. Tyto analýzy hrozeb, známé jako ESET APT Reports PREMIUM, pomáhají organizacím, které mají za úkol chránit občany, kritickou národní infrastrukturu a hodnotná aktiva před kyberútoky ze strany kriminálních skupin a státem řízených útoků. Tato zpráva obsahuje pouze zlomek informací poskytovaných zákazníkům prémiových zpráv.

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 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-vydal-zpravu-o-aktivitach-staty-podporovanych-utocniku-nejvice-operaci-bylo-spojeno-s-ruskem