Hackerské skupiny napojené na Čínu zacílily na EU, terčem skupin napojených na Rusko zůstává Ukrajina

9.11.2023 - Rita Gabrielová, Lucie Mudráková | ESET software

Společnost ESET vydala zprávu ESET APT Activity Report, ve které se věnuje nejnovějším informacím o aktivitách dlouhodobě sledovaných útočných skupin napojených na národní státy, především na Čínu, Severní Koreu, Rusko a Írán. Podle posledních zjištění se útočné skupiny v několika posledních měsících zaměřovaly na zneužívání zranitelností celé řady široce využívaných programů a mezi jejich cíli nechybí organizace zemí Evropské unie, včetně České republiky. Zpráva se také zabývá přetrvávajícími kampaněmi na cíle v EU, za nimiž stojí skupiny napojené na Čínu, anebo vývojem kybernetické války na Ukrajině, která se z fáze sabotáže přesunula ke špionáži.

Společnost ESET vydala nejnovější zprávu o aktivitách vybraných APT skupin, které její kyberbezpečnostní experti pozorovali, zkoumali a analyzovali od dubna do konce září 2023. APT neboli Advanced Persistent Threat je označení pro skupinu útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby a bývají napojeni na národní státy.

„Ačkoli jsou útoky APT skupin vysoce cílené a tím se odlišují od útoků, jejichž cílem je masově zasáhnout co největší počet obětí, v současném globálním prostředí kybernetických hrozeb se nevyhýbají ani České republice," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET. „Ve sledovaném období to potvrdila například srpnová spearphishingová kampaň APT skupiny Sednit napojené na Rusko, která kromě Ukrajiny a Polska cílila i na Česko. Skupina využila zranitelnosti nultého dne v aplikaci Microsoft Outlook, která byla zveřejněna již v březnu 2023," říká Šuman.

V aktuální zprávě tak na sebe strhly pozornost právě APT skupiny, které zneužívaly známé zranitelnosti k exfiltraci dat z vládních subjektů nebo spřízněných organizací. Ve zprávě bezpečnostní experti upozorňují také na přetrvávající kampaně skupin napojených na Čínu v EU a na vývoj ruské kybernetické války na Ukrajině.

Také další skupiny z různých monitorovaných geografických oblastí zneužívaly zranitelnosti, například v programu WinRAR, serverech Microsoft Exchange a IIS.

APT skupiny Sednit a Sandworm, které jsou napojeny na Rusko, Konni, která je napojena na Severní Koreu, a skupiny Winter Vivern a SturgeonPhisher, které zatím nejsou geograficky zařazeny, zneužily zranitelnosti v programech a softwarových nástrojích WinRAR (Sednit, SturgeonPhisher a Konni), Roundcube (Sednit a Winter Vivern), Zimbra (Winter Vivern) a Outlook pro operační systém Windows (Sednit) k útokům na různé vládní organizace nejen na Ukrajině, ale i v Evropě a Střední Asii.

„Skupina Sednit dále zneužila také zranitelnosti v archivátoru WinRAR, která umožňovala útočníkům spustit libovolný kód. Útočníci lákali v tomto případě oběti z řad politických subjektů v EU a na Ukrajině na otevření přílohy e-mailu, kterou vydávali za program schůzky Evropského parlamentu. Zranitelnosti široce využívaných programů jsou velkým rizikem – je to nekončící závod o to, za jak dlouho se podaří zranitelnost odhalit a opravit a jak dlouho do jejího odhalení ji budou moci útočníci případně zneužívat," dodává Šuman z ESETu.

Pokud jde o skupiny napojené na Čínu, GALLIUM pravděpodobně využívala slabiny v serverech Microsoft Exchange nebo IIS, čímž rozšířila své zaměření z telekomunikačních operátorů na vládní organizace po celém světě. Skupina MirrorFace pravděpodobně využívala zranitelnosti ve službě online úložiště Proself a skupina TA410 pak chyby v aplikačním serveru Adobe ColdFusion.

Hlavním cílem skupin napojených na Rusko zůstala Ukrajina. Analytici z ESETu zde objevili nové verze známých wiperů RoarBat a NikoWiper a nový wiper, který pojmenovali SharpNikoWiper a který nasadila skupina Sandworm. Malware typu wiper monitoruje ESET již od začátku samotné ruské invaze.

Zpráva také upozorňuje, že zatímco skupiny jako Gamaredon, GREF a SturgeonPhisher se zaměřují na uživatele Telegramu a snaží se exfiltrovat informace nebo alespoň některá metadata související s Telegramem, APT skupina Sandworm tuto službu aktivně využívá k propagaci svých kybernetických sabotáží. Nejaktivnější skupinou na Ukrajině nadále zůstávala Gamaredon, která výrazně vylepšila své možnosti sběru dat přepracováním svých stávajících nástrojů a nasazením nových.

Bezpečnostní experti odhalili činnost také tří dosud neznámých skupin napojených na Čínu: DigitalRecyclers, která opakovaně kompromitovala vládní organizaci v EU; TheWizards, která prováděla útoky typu adversary-in-the-middle; a PerplexedGoblin, která se zaměřovala na další vládní organizaci v EU.

Skupiny napojené na Írán a Blízký východ podle závěrů zprávy pokračovaly ve své rozsáhlé činnosti a zaměřovaly se především na špionáž a krádež dat organizací v Izraeli. Skupina MuddyWater, která je spojena s Íránem, se zaměřila na neidentifikovaný subjekt v Saúdské Arábii, přičemž po prvotní kompromitaci nasadila také tzv. payload, tedy část škodlivého kódu, která je navržena k provedení škodlivé aktivity v cílovém systému. To naznačuje možnost, že tato skupina slouží k vývoji přístupu pro pokročilejší APT skupiny.

Aktivní byla i skupina OilRig, u které bezpečnostní specialisté z ESETu v dubnu objevili novou sadu nástrojů. Tu skupina nasadila proti několika obětem v Izraeli. Začátkem července potom u této skupiny pozorovali novou variantu zadních vrátek nazvanou Mango, která se poprvé objevila už na počátku roku 2023.

Skupiny napojené na Severní Koreu se nadále zaměřovaly na Japonsko, Jižní Koreu a na ní zaměřené subjekty a používaly ve svých operacích pečlivě připravené spearphishingové e-maily. Nejaktivnějším pozorovaným schématem APT skupiny Lazarus byla operace DreamJob, která lákala oběti na falešné nabídky lukrativních pracovních pozic. Tato skupina byla také schopna vytvářet malware pro všechny hlavní desktopové platformy.

Aktuální zpráva ESET APT Activity Report nabízí závěry analýz bezpečnostních expertů z ESETu za období od dubna 2023 do konce září 2023. Zprávy obsahují pouze zlomek dat kyberbezpečnostního zpravodajství poskytovaného zákazníkům odebírajícím plné znění ESET APT Reportu.

Analytici ze společnosti ESET připravují hloubkové technické zprávy a pravidelné aktualizace aktivit s podrobnými informacemi o konkrétních APT skupinách v podobě ESET APT Reports PREMIUM, které pomáhají organizacím, jejichž úkolem je chránit občany, kritickou národní infrastrukturu a vysoce cenná aktiva před kybernetickými útoky řízenými kyberzločinci či národními státy. Detailní popisy aktivit obsažených v tomto dokumentu byly proto dříve poskytovány výhradně našim prémiovým zákazníkům. Více informací o službě ESET APT Reports PREMIUM, která poskytuje kvalitní, strategické a taktické zpravodajské informace o kybernetických hrozbách, je k dispozici na webových stránkách ESET Threat Intelligence.

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 produktů 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-hackerske-skupiny-napojene-na-cinu-zacilily-na-eu-tercem-skupin-napojenych-na-rusko-zustava-ukr