ESET odhalil dezinformační kampaně na Ukrajině, stopy útočníků vedou do Ruska

21.2.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Bezpečnostní experti z kyberbezpečnostní společnosti ESET odhalili PSYOPs operaci obsahující dezinformace o válce na Ukrajině, kterou útočníci s vazbami na Rusko šíří prostřednictvím e-mailového spamu. Během dvou vln manipulativních e-mailů se útočníci pokusili ovlivnit a demoralizovat ukrajinské obyvatele. V souvislosti s dezinformačními e-maily pak experti objevili další spearphishingovou kampaň, která byla zaměřena na ukrajinskou obrannou společnost a na agenturu Evropské unie. Na základě objevených podobností v síťové infrastruktuře vše nasvědčuje tomu, že spolu oba typy útoků souvisejí. Operace Texonto, jak jsou phishingové a dezinformační útoky společně nazvány, připomínají aktivity kyberšpionážní skupiny Callisto napojené na Rusko. Dosavadní důkazy však zatím nepotvrdily, že by za operací stála konkrétní útočná skupina. Bezpečnostní experti momentálně neevidují podobnou operaci v České republice, riziko přímé dezinformační spamové kampaně dle nich však nelze do budoucna vyloučit.

Bezpečnostní experti z ESETu nově odhalili operaci Texonto, psychologickou a informační (tzv. PSYOPs) útočnou kampaň, během které útočníci využívají e-mailový spam jako hlavní metodu šíření hrozby mezi svými oběťmi. Během dvou vln rozesílání těchto e-mailů se útočníci navázaní na Rusko pokusili ovlivnit ukrajinské obyvatele tvrzeními, která měla vést k domnění, že Rusko vyhrává válku na Ukrajině.

První vlna útoku se uskutečnila v listopadu 2023 a druhá vlna poté na konci prosince 2023. Obsahem e-mailů byly zprávy o přerušení dodávek tepla, nedostatku léků a jídla, což jsou témata typicky využívaná ruskou propagandou. V říjnu 2023 bezpečnostní experti objevili také spearphishingovou kampaň zacílenou na ukrajinskou obrannou společnost a v listopadu poté na agenturu Evropské unie, při které útočníci využili napodobeninu přihlašovací stránky ke službě Microsoft Office 365. Cílem útočníků bylo v tomto případě odcizit účty k této službě. Na základě podobností v síťové infrastruktuře, které se objevily během těchto dezinformačních a phishingových kampaní, se bezpečnostní experti z ESETu domnívají, že jsou spolu jednotlivé útoky propojeny.

„Od začátku války na Ukrajině se útočné skupiny napojené na Rusko, jako například skupina Sandworm, zaměřily na zničení ukrajinské IT infrastruktury za použití wiperů. Wipery jsou škodlivé kódy určené nikoliv k dosažení finančního zisku, což je v dnešní době hlavním motivem kyberkriminality, ale jsou přímým nástrojem k destrukci. V posledních několika měsících jsme byli zase svědky nárůstu kyberšpionážních operací pod vedením neblaze proslulé útočné skupiny Gamaredon. Operace Texonto pak ukazuje další rozměr využití kyberprostoru ve válce," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET.

„Tento typ přímých operací, jako je Texonto, v současnosti neevidujeme v Česku. Spíše zde vidíme dezinformační kampaně prostřednictvím třetích osob, dezinformačních webů nebo šíření nepravdivých informací na sociálních sítích. Větší spamovou kampaň ovšem nelze do budoucna vyloučit ani v případě České republiky, zvlášť, pokud by se útočným skupinám naskytlo správné téma, kterým obecně bývají například volby," dodává Šuman.

„Kombinace kybernetické špionáže, informačních operací a falešných zpráv o léčivech připomíná aktivity skupiny Callisto, známou a na Rusko napojenou kyberšpionážní skupinu. Někteří její členové byli v prosinci 2023 dokonce obžalováni ministerstvem spravedlnosti USA. Oběťmi skupiny Callisto

jsou vládní činitelé, zaměstnanci think tanků nebo organizací zaměřených na armádní oblast. Skupina napadá oběti prostřednictvím spearphishingových webových stránek, které jsou navrženy tak, aby napodobovaly známé poskytovatele cloudových služeb," říká Šuman.

„Skupina Callisto je ale také podepsána pod dezinformačními kampaněmi, například únikem dokumentů těsně před britskými volbami v roce 2019, a svou starou síťovou infrastrukturu využívá k vytváření falešných domén se zdravotnickou tématikou. Nicméně i přes několik významných podobností operace Texonto s operacemi skupiny Callisto jsme zatím nenašli důkazy o využití stejných technologií, a proto operaci Texonto nemůžeme v tuto chvíli připsat žádné konkrétní útočné skupině," dodává Šuman z ESETu.

Na základě získaných informací o TTPs (techniky, taktiky a postupy útočníka), zacílení na oběti a šíření zpráv je ale podle ESETu pravděpodobné, že útočníci jsou napojeni na Rusko.

Mailový server využívaný útočníky k zasílání manipulativních e-mailů byl znovu využit po dvou týdnech od zjištěných útočných kampaní k rozeslání dalšího lékárenského spamu, který se označuje jako tzv. Canadian pharmacy spam. Tento typ spamu je v ruské kyberkriminální komunitě dlouhodobě velmi populární.

Podrobnějším zkoumáním pak ESET odhalil jména domén, které jsou součástí operace Texonto, a odkazují například i na jméno Alexeje Navalného. Operace Texonto tak pravděpodobně obsahuje také spearphishingové či informační kampaně zaměřené na ruské disidenty a podporovatele zesnulého vůdce opozice.

Cílem první vlny dezinformačních e-mailů bylo zasít pochybnosti mezi ukrajinské obyvatele, například zprávami o přerušení dodávek tepla během letošní zimy. Jiné e-maily, které měly působit jako zprávy z ministerstva zdravotnictví, obsahovaly zprávy o nedostatku léků. Podle zjištěných informací e-maily neobsahovaly žádné nebezpečné odkazy ani malware, jejich cílem tak bylo pouze šířit dezinformace. Jedna z domén například napodobovala ukrajinské ministerstvo zemědělství a obsahem zpráv bylo doporučení obyvatelům Ukrajiny nahradit nedostupné léky bylinnými alternativami. V jiném e-mailu mělo ministerstvo doporučovat konzumaci tzv. „holubího rizota". Dokumenty byly pravděpodobně vytvořeny s cílem vzbudit pobouření mezi čtenáři a demoralizovat je. Všechny tyto falešné zprávy se řadí mezi známá témata ruské propagandy. Jejich cílem je přesvědčit ukrajinské obyvatele, že v zemi zmítané válkou je nedostatek jídla, léků a dodávek tepla.

Zhruba měsíc po první vlně dezinformačních e-mailů ESET zaznamenal druhou psychologickou e-mailovou kampaň zaměřenou nejen na ukrajinské obyvatele, ale také na ostatní evropské země. Cílila tentokrát na různé oběti, od ukrajinské vlády až po výrobce bot v Itálii. Na základě dat společnosti ESET obdrželo tyto e-maily několik stovek lidí. Ve druhé vlně manipulativních e-mailů se objevily například zprávy s doporučeními na amputaci nohou či rukou, aby se lidé vyhnuli odvodům. Tyto zprávy měly opět charakter PSYOPs operací během válečného konfliktu.

Bezpečnostní analytici společnosti ESET objevili 23. února 2022 ve večerních hodinách nový malware označovaný jako HermeticWiper. Šlo o škodlivý kód typu data wiper, který maže uživatelská data a který byl během středy v předvečer invaze použit ke kybernetickým útokům na řadu významných organizací na Ukrajině. V den invaze proběhl útok za použití malwaru IsaacWiper, který mířil na ukrajinskou vládní síť. Kromě vládních cílů byly útoky wiperem v dalších dnech detekovány také v případě organizací z řad médií. Později byly popsány další škodlivé kódy – worm (červ) HermeticWizard, který napomáhal šíření wiperu uvnitř lokálních sítí, či ransomware HermeticRansom, který byl použit jako zastírací manévr a měl od hlavního útoku odvést pozornost.

Velkým tématem se ihned po invazi staly spamové a phishingové kampaně. Prostřednictvím

falešných sbírek začali podvodníci zneužívat solidaritu lidí, kteří chtěli podpořit oběti konfliktu. V březnu 2022 pak společnost ESET identifikovala další malware CaddyWiper zaměřující se na ukrajinské finanční instituce. V dubnu pak bezpečnostní experti z ESETu odhalili útok za použití wiperu CaddyWiper a již dříve detekovaného malwaru Industroyer, který byl použit k přerušení dodávky elektřiny na Ukrajině v roce 2016. Podle zjištění byla autorem útoku skupina Sandworm s vazbami na ruskou zpravodajskou službu GRU. Cílem byla opět významná energetická společnost distribuující elektřinu na území Ukrajiny.

Další technické informace o operaci Texonto najdete na webu www.welivesecurity.com.

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 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-odhalil-dezinformacni-kampane-na-ukrajine-stopy-utocniku-vedou-do-ruska