Čína a Severní Korea sledují nové cíle a zároveň zdokonalují kybernetické schopnosti

blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea

September 7, 2023

V minulém roce Čína zdokonalila novou schopnost automatického generování obrázků, které může použít pro operace vlivu, jejichž cílem je napodobit americké voliče napříč politickým spektrem a vytvořit kontroverze po rasové, ekonomické a ideologické linii. Tato nová schopnost je poháněna umělou inteligencí, která se pokouší vytvářet vysoce kvalitní obsah, který by se mohl šířit po sociálních sítích v USA a dalších demokraciích. Tyto obrázky jsou s největší pravděpodobností vytvářeny něčím, čemu se říká generátory obrázků poháněné difúzí, které využívají AI nejen k vytváření působivých obrázků, ale také se je učí časem vylepšovat.

Centrum pro analýzu hrozeb společnosti Microsoft (MTAC) dnes vydává Sofistika, rozsah a rozsah: Šířka a efektivita digitálních hrozeb z východní Asie je součástí pokračující série zpráv o hrozbách, které představují ovlivňování a kybernetická aktivita, a identifikují konkrétní sektory a regiony se zvýšeným rizikem.

Pozorovali jsme herce spřízněné s Čínou, kteří využívají vizuální média generovaná umělou inteligencí v široké kampani, která se z velké části zaměřuje na politicky rozdělující témata, jako je násilí se zbraněmi a očerňování amerických politických osobností a symbolů. Tato technologie vytváří poutavější obsah než trapné digitální kresby a koláže fotografií používané v předchozích kampaních. Můžeme očekávat, že Čína bude tuto technologii v průběhu času dále zdokonalovat, i když se teprve uvidí, jak a kdy ji ve velkém nasadí.

Jak Microsoft poznamenal v naší nedávné zprávě Governing AI: Blueprint for the Future , instituce veřejného a soukromého sektoru se musí kolektivně zabývat zbrojením technologií, včetně AI, ze strany kybernetických a ovlivňovaných aktérů hrozeb. Podáváme zprávy o digitálních hrozbách, které odhalíme – včetně použití umělé inteligence –, abychom informovali tvůrce politik, bezpečnostní odborníky a veřejnost o jakýchkoli současných nebo vznikajících hrozbách, které nové technologie mohou představovat pro integritu informací a demokracii. Budeme pokračovat ve sdílení našich znalostí a vyzveme partnery, aby tak činili také, jako součást našeho širšího plánu na podporu transparentnosti a vedení řízení AI.

Ve svých kybernetických operacích několik čínských státních aktérů zaměřených na hrozby zaměřilo kybernetické útoky v oblasti Jihočínského moře, provádělo shromažďování zpravodajských informací a spouštění malwaru proti regionálním vládám a průmyslovým odvětvím. Další aktéři se zaměřili na americký obranný průmysl a americkou infrastrukturu a hledali konkurenční výhody k posílení strategických vojenských cílů.

Počínaje květnem 2023 přistupoval Storm-0558, čínský hrozebný subjekt, k e-mailovým účtům zákazníků Microsoftu přibližně 25 organizací včetně amerických a evropských vládních subjektů. Microsoft se domnívá, že tato aktivita byla pravděpodobně prováděna pro účely špionáže a úspěšně tuto kampaň zablokovala.

Zpráva také podrobně popisuje, jak Čína pokračuje ve svém globálním úsilí o šíření státem sponzorované propagandy a zjemnění obrazu země v zahraničí. Čínská vláda investuje prostředky do zasílání zpráv publiku ve více jazycích, na více platformách a zároveň vyvíjí své techniky. Víme například, že Čína zaměstnává více než 230 zaměstnanců státních médií a přidružených společností, kteří se maskují jako nezávislí ovlivňovatelé sociálních médií na všech hlavních západních platformách sociálních médií.

Tito influenceři, kteří jsou rekrutováni, trénováni, podporováni a financováni organizací China Radio International (CRI) a dalšími čínskými státními sdělovacími prostředky, odborně šíří lokalizovanou propagandu ČKS, která dosahuje smysluplného zapojení s publikem po celém světě a dosahuje kombinované sledovanosti nejméně 103. milionů lidí na různých platformách hovořících alespoň 40 jazyky.

Zatímco skupiny hrozeb se sídlem v Číně nadále rozvíjejí a využívají působivé kybernetické schopnosti a IO operace, nezaznamenali jsme, že by Čína kombinovala kybernetickou oblast a vliv – na rozdíl od Íránu a Ruska, které se pravidelně zapojují do kampaní proti hackerům a únikům.

Kromě toho, co jsme pozorovali z Číny, je Severní Korea schopnou kybernetickou hrozbou, která se zaměřuje na shromažďování zpravodajských informací a krádeže kryptoměny potřebné k vytváření příjmů pro stát. Několik severokorejských aktérů ohrožení se zaměřilo na námořní a loďařský sektor, což naznačuje, že jde o oblast s vysokou prioritou severokorejské vlády. Kromě toho se několik severokorejských aktérů hrozeb nedávno zaměřilo na ruskou vládu a obranný průmysl – pravděpodobně kvůli shromažďování zpravodajských informací – a současně poskytovali materiální podporu Rusku v jeho válce na Ukrajině.

Zpráva se také zaměřuje na očekávané budoucí kroky Číny a Severní Koreje v nadcházejících měsících, protože rostoucí geopolitické napětí pohání nové priority hrozeb a nepřátelské strategie. S nadcházejícími volbami v roce 2024 pravděpodobně zůstanou hlavními prioritami Číny Tchaj-wan a Spojené státy.

Žádná technologická platforma, včetně té Microsoft, není dokonalá. Ale vzhledem k tomu, že aktéři národních států pokračují v zaměřování se na zranitelná místa a rozšiřování škodlivých narativů po celém světě, věříme, že je životně důležité pokračovat ve sdílení zpravodajských informací, jako je tato zpráva, a ve zvyšování meziodvětvové spolupráce v těchto důležitých otázkách.

Poznámka editora: Společnost Microsoft dnes v rámci probíhající série zveřejnila Sophistication, scale and scale: Digitální hrozby z východní Asie nabývají na šíři a efektivitě . Tyto pololetní aktualizace národních státních aktérů slouží k varování našich zákazníků a globální komunity před hrozbou, kterou představují operace vlivu a kybernetické aktivity, a identifikují konkrétní sektory a regiony se zvýšeným rizikem. Podívejte se na naše předchozí zprávy o Rusku a Íránu .

Štítky: kybernetické útoky , kybernetická bezpečnost , kybernetická válka , Centrum pro analýzu digitálních hrozeb , MTAC , Ukrajina