Opláchněte a opakujte: Írán urychluje své operace kybernetického vlivu po celém světě

blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat

May 2, 2023

Írán nadále představuje významnou hrozbu a své tradiční kybernetické útoky nyní doplňuje o novou příručku, která využívá kybernetické vlivové operace (IO) k dosažení svých geopolitických cílů.

Společnost Microsoft zjistila, že se tyto snahy od června 2022 rychle zrychlují. V loňském roce jsme íránské vládě připsali 24 unikátních kybernetických operací vlivu – včetně 17 od června do prosince – ve srovnání s pouhými sedmi v roce 2021. Odhadujeme, že většina íránských kybernetických operací vlivové operace řídí Emennet Pasargad – kterého sledujeme jako Cotton Sandstorm (dříve

NEPTUNIUM) – íránský státní aktér sankcionovaný ministerstvem financí USA za jejich pokusy podkopat integritu prezidentských voleb v roce 2020 v USA.

I když se íránské techniky mohly změnit, jeho cíle nikoli. Tyto operace se i nadále zaměřují na Izrael, prominentní osobnosti a skupiny íránské opozice a protivníky státu v Teheránském zálivu. Obecněji řečeno, Írán v období od října 2022 do března 2023 nasměroval téměř čtvrtinu (23 %) svých kybernetických operací proti Izraeli, přičemž tíhu těchto snah nesly také Spojené státy, Spojené arabské emiráty a Saúdská Arábie.

Íránští kybernetičtí aktéři stáli v popředí kybernetické IO, ve kterém kombinují útočné kybernetické operace s operacemi s mnohostranným vlivem, aby podpořily geopolitické změny v souladu s cíli režimu. Mezi cíle její kybernetické IO patří úsilí o posílení palestinského odporu, podněcování nepokojů v Bahrajnu a boj proti pokračující normalizaci arabsko-izraelských vazeb, se zvláštním zaměřením na rozsévání paniky a strachu mezi izraelskými občany.

Írán také přijal kybernetickou IO, aby podkopal dynamiku celonárodních protestů únikem informací, které mají za cíl uvést do rozpaků prominentní představitele opozice režimu nebo odhalit jejich „zkorumpované“ vztahy.

Většina těchto operací má předvídatelnou příručku, ve které Írán používá kybernetickou osobnost k propagaci a zveličování málo sofistikovaného kybernetického útoku, než zdánlivě nesouvisející neautentické online persony zesílí a často dále rozšíří dopad útoků pomocí jazyka cílového publika. Nové techniky íránského vlivu zahrnují jejich používání SMS zpráv a předstírání identity obětí ke zvýšení účinnosti jejich zesílení.

Toto je několik postřehů v nové zprávě Microsoft Threat Intelligence o íránském kybernetickém IO. Zpráva zdůrazňuje, jak Írán využívá tyto operace k efektivnější odvetě proti vnějším a vnitřním hrozbám.

Zabývá se také tím, jaké akce je můžeme vidět v následujících měsících, včetně vyšší rychlosti, s jakou zprovozňují nově hlášené exploity.

Vzhledem k tomu, že některé íránské skupiny hrozeb přešly na kybernetické IO, zaznamenali jsme odpovídající pokles v používání ransomwaru nebo stěračů v Íránu, kvůli nimž se v posledních dvou letech staly hojnými .

Zároveň zůstává budoucí hrozba stále ničivějších íránských kybernetických útoků, zejména proti Izraeli a Spojeným státům, protože některé íránské skupiny pravděpodobně hledají možnosti kybernetického útoku proti průmyslovým kontrolním systémům. Íránské kybernetické útoky a vlivové operace budou pravděpodobně i nadále zaměřeny na odvetu proti zahraničním kyberútokům a vnímané podněcování protestů uvnitř Íránu.

Microsoft investuje do sledování a sdílení informací o íránských kybernetických IO, aby se zákazníci a demokracie po celém světě mohly chránit před útoky. Budeme zveřejňovat pololetní aktualizace o těchto a dalších národních aktérech, abychom varovali naše zákazníky a globální komunitu před hrozbou, kterou takové operace představují, a identifikujeme konkrétní sektory a regiony se zvýšeným rizikem.

Štítky: kybernetický vliv , kybernetické útoky , kybernetická bezpečnost , Digital Threat Analysis Center , Írán , Microsoft Threat Intelligence Center , MSTIC , hrozba