Probíhající ruské kybernetické útoky zaměřené na Ukrajinu

blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard

June 14, 2023

Týmy Microsoftu o hrozbách sledovaly vlnu kybernetických útoků od herce, kterému říkáme Cadet Blizzard a který je spojen s ruskou GRU. Tyto útoky, které začaly v únoru 2023, byly zaměřeny na vládní agentury a poskytovatele IT služeb na Ukrajině. Cadet Blizzard nyní také můžeme připsat destruktivní útoky stěračů WhisperGate proti Ukrajině zjištěné společností Microsoft v lednu 2022 před ruskou invazí.

Cadet Blizzard obvykle porušuje své cíle pomocí ukradených přihlašovacích údajů k získání přístupu k internetovým serverům, které jsou umístěny na perimetrech sítě organizace. Jakmile je uvnitř, snaží se zachovat přístup pomocí široce dostupných nástrojů nazývaných webové shelly, které lze zakoupit jako běžné sady a upravit je. Poté používá techniky „žití ze země“ – to znamená, že běžně používá legitimní příkazy, nikoli malware, k laterálnímu

pohybu v sítích svých cílů a zároveň získává přístup k více informacím nebo narušuje sítě, pokud se tak rozhodne. Používání technik „živobytí ze země“ mu pomáhá skrývat se v legitimním síťovém provozu, což ztěžuje jeho odhalování.

Cadet Blizzard je aktivní sedm dní v týdnu a své operace prováděl mimo pracovní dobu svých primárních cílů, kdy je méně pravděpodobné, že bude jeho aktivita odhalena. Kromě Ukrajiny se zaměřuje také na členské státy NATO zapojené do poskytování vojenské pomoci Ukrajině.

Co je možná nejzajímavější na tomto herci, je jeho relativně nízká úspěšnost ve srovnání s jinými herci spřízněnými s GRU, jako jsou Seashell Blizzard (Iridium) a Forrest Blizzard (Strontium). Útoky stěračů z února 2022 připisované samotnému Seashell Blizzard zasáhly více než 200 systémů zahrnujících více než 15 organizací, zatímco útok WhisperGate z ledna 2022 Cadet Blizzard zasáhl řádově méně systémů a přinesl poměrně mírný dopad, přestože byl vycvičen k ničení sítí svých protivníků. na Ukrajině. Aktivita Cadet Blizzard vzrostla mezi lednem a červnem 2022, rozplynula se a znovu se objevila na začátku roku 2023. Novější kybernetické operace Cadet Blizzard, i když občas úspěšné, podobně nedokázaly dosáhnout dopadu operací prováděných jeho protějšky GRU.

Skromné výsledky přinesla i práce vlivových operací skupiny. Na začátku roku 2022 úspěšně znehodnotila řadu ukrajinských webů. Kanál „Free Civilian“ Telegram, který Cadet Blizzard používá k distribuci informací získaných z operací hackerů a úniků, však měl k únoru 2023 pouze 1,3 tisíc sledujících, přičemž příspěvky získaly v době od roku maximálně tucet reakcí. publikace, což znamená nízkou interakci s uživatelem.

Věříme, že Cadet Blizzard funguje od roku 2020. Kromě Ukrajiny a členských států NATO se zaměřil na řadu organizací v Evropě a Latinské Americe.

I když to nebyl nejúspěšnější ruský herec, Cadet Blizzard zaznamenal v poslední době určitý úspěch. Jedinečná viditelnost Microsoftu do jejich operací nás motivovala ke sdílení informací s bezpečnostním ekosystémem a zákazníky, abychom zvýšili viditelnost a ochranu před jejich útoky. Jako vždy jsme upozornili zákazníky, kteří se stali terčem útoku nebo byli napadeni, a dnes jsme sdíleli podrobné technické informace , které pomohou bezpečnostní komunitě identifikovat a bránit se proti útokům tohoto aktéra.

Štítky: kybernetický vliv , kybernetické útoky , Centrum pro analýzu digitálních hrozeb , digitální hrozby , Ukrajina