'Soubory Vulkan': Uniklé dokumenty odhalují ruské strategie kybernetické války

interestingengineering.com/culture/vulkan-files-leaked-papers-russias-cyberwarfare

31. března 2023

Rusko údajně spolupracovalo s moskevským dodavatelem obrany NTC Vulkan na provádění kybernetických útoků a šíření dezinformací.

Podle uniklých dokumentů, o nichž ve čtvrtek informovaly mediální zdroje, je zdůrazněno několik programů a databází, které by ruským zpravodajským agenturám a hackerským organizacím umožnily identifikovat bezpečnostní chyby, plánovat útoky a manipulovat s online aktivitou.

Viz také

"Lidé by měli znát nebezpečí, které to přináší," řekl informátor, který dokumenty unikl.

"Kvůli událostem na Ukrajině jsem se rozhodl tuto informaci zveřejnit. Společnost dělá špatné věci a ruská vláda je zbabělá a chybná."

"Jsem naštvaný kvůli invazi na Ukrajinu a hrozným věcem, které se tam dějí. Doufám, že tyto informace využijete k tomu, abyste ukázali, co se děje za zavřenými dveřmi," dodal zdroj.

Mezi zmíněnými byly programy, které podporovaly dezinformace sociálních médií a školení na dálku, aby narušovaly systémy, které regulují železniční, leteckou a námořní dopravu.

Zdroj uniklých dokumentů není znám, ale byly poskytnuty německému reportérovi po ruském útoku na Ukrajinu, tvrdí zprávy.

O data a další informace se zdroj později podělil s mnichovským investigativním startupem Paper Trail Media.

Novináři z 11 mediálních organizací, včetně *The Guardian* , *Washington Post* a *Le Monde* , zkoumali data několik měsíců jako součást skupiny organizované Paper Trail Media a Der Spiegel.

Cílem hackerů byla jaderná elektrárna

Záznamy poskytují jedinečný pohled na tajná obchodní jednání ruských vojenských a zpravodajských služeb, včetně výroby softwaru pro nechvalně proslulou elitní hackerskou skupinu Sandworm.

Nejoblíbenější

Sandworm je obviněn, že je zodpovědný za výpadky elektřiny na Ukrajině, zasahování do zahajovacího ceremoniálu zimních olympijských her v roce 2018 a vydání NotPetya, nejničivějšího malwaru v historii.

Neexistuje žádný konkrétní důkaz, že systémy byly nasazeny Ruskem nebo použity při konkrétním narušení, přestože zástupci pěti západních zpravodajských služeb a řady nezávislých firem zabývajících se kybernetickou bezpečností tvrdí, že věří, že dokumenty jsou autentické, uvádí zpráva Washington Post . .

Uniklé dokumenty však odhalují platby za práci prováděnou Vulkanem pro četné výzkumné ústavy, včetně ruských zpravodajských služeb.

Dokumenty, které zahrnují roky 2016 až 2021 a zahrnují pokyny, technické specifikace, interní korespondenci od korporace, finanční záznamy a smlouvy, dokládají šíři zakázky, kterou Moskva outsourcovala.

Podle *WP* NTC Vulkan vytvořil software pro Rusko, včetně aplikací, které generují falešné profily na sociálních sítích, a také aplikací, které dokážou najít a sestavit seznamy zranitelností v počítačových systémech po celém světě, které by mohly být zneužity.

Kromě toho má rozhraní pro řadu projektů, jako je Amezit a Skan, které identifikují potenciální cíle hackerů, včetně švýcarského ministerstva zahraničí a jaderné elektrárny.

Dokumenty hovoří o „uživatelském scénáři“, ve kterém by hackerský tým našel zranitelné routery v Severní Koreji, aby mohl zahájit kybernetický útok.

„Tyto dokumenty naznačují, že Rusko vidí útoky na civilní kritickou infrastrukturu a manipulaci se sociálními médii jako jednu a tu samou misi, která je v podstatě útokem na vůli nepřítele bojovat,“ řekl John Hultquist, viceprezident pro analýzu zpravodajských služeb společnosti Mandiant pro kybernetickou bezpečnost. , která na žádost konsorcia přezkoumala některé materiály.

Přestože Vulkan nereagoval na žádosti *Washington Post* o komentář , dokumenty poskytují pohled na cíle ruského státu, který stejně jako ostatní velké mocnosti, jako jsou Spojené státy, touží po růstu a zlepšení své schopnosti provádět kybernetické útoky na ve velkém měřítku a vysokou rychlostí.

Anonymní zdroj „5000stránkového dokumentu“ podle zprávy *The Guardian* mluvil s reportérem prostřednictvím šifrované chatovací aplikace a odmítl uvést své jméno s tím, že z bezpečnostních důvodů musí zmizet „jako duch“.

1. Domov
2. Kultura

ZOBRAZIT KOMENTÁŘ (0)