Konflikt na Ukrajině se stává největším veletrhem práce pro kyberzločince

infokuryr.cz/n/2023/01/07/konflikt-na-ukrajine-se-stava-nejvetsim-veletrhem-prace-pro-kyberzlocince

kuryr 7. ledna 2023

Konflikt na Ukrajině zhoršuje už tak napjatou situaci v kyberprostoru, píše expert na informační bezpečnost Richard Werner v článku pro Der Tagesspiegel. Kyberzločinecké společnosti jej využívají k náboru odhodlaných mladých lidí, které láká možnost vydělat na konfliktu více peněz než na právním poli. Nárůst počtu kyberzločinců vám ani po skončení bojů nedovolí s investicemi vydechnout, domnívá se expert.

Na pozadí konfliktu na Ukrajině se již tak napjatá situace v kyberprostoru vyostřuje. Panují obavy, že změny mohou zasáhnout i Německo. Zatím však došlo jen k drobným incidentům. Německý Spolkový úřad pro informační bezpečnost například od konce dubna opakovaně zaznamenává DDoS útoky hacktivistů, které se však ve většině případů podařilo odrazit, píše v článku pro Der Tagesspiegel odborník na kybernetickou bezpečnost Richard Werner.

Nejpozoruhodnější byl útok na satelitní síť KA-SAT amerického poskytovatele Viasat. Ruští hackeři se podle Wernera snažili vážně narušit komunikaci mezi Ukrajinou a partnery v NATO. Centra dálkového ovládání ztratila v důsledku kybernetického útoku kontrolu nad tisíci větrných turbín po celé Evropě. 5800 z nich se nachází v Německu.

Nepokoje na druhou stranu vyvolali i němečtí hacktivisté: v březnu skupina Anonymous zaútočila na servery dceřiné společnosti ruského ropného gigantu Rosněft. Podle skupiny hackeři zachytili 20 terabajtů dat. Z bezpečnostních důvodů musela společnost dočasně odstavit své systémy.

Kdo jsou tito útočníci, kteří vstoupili na scénu kybernetické kriminality s vypuknutím konfliktu? *„Na jedné straně vidíme hacktivisty, kteří jednají z nějakých ideálů nebo politických důvodů. Na rozdíl od jiných kyberzločinců nesledují žádné finanční zájmy, ale bojují za „spravedlivou věc" z jejich pohledu. Útočí přitom jak na své přímé odpůrce, tak na každého, koho považují za své příznivce. Svým jednáním chtějí hacktivisté upoutat pozornost, odhalit firmy, sabotovat je nebo narušit důležité systémy. Často nemají kyberzločineckou minulost,* " píše Werner.

Expert pokračuje: *„Navíc se objevila nová kategorie hackerů, kterým říkáme kybernetické žoldáky. Jedná se o profesionální kyberzločince, kteří nabízejí své služby vládám nebo jiným skupinám. Méně se starají o své politické přesvědčení a více* o *své vlastní zisky. Jejich výplata však nespočívá v pytli zlata v klasickém slova smyslu, ale v nevyřčené dohodě: dokud hackeři budou stát podporovat a neútočit na žádné cíle ve své zemi, bude tolerovat jejich kyberzločinecké machinace.*

I kyberzločinecké firmy potřebují schopné *„profesionály"* , aby uspěly na trhu. Využívají konflikt na Ukrajině jako příležitost k náboru motivovaných mladých lidí. Hacktivisté mají možnost učit se od těch nejlepších.

Pro mnohé mohou stále převažovat politické zájmy. Proč ale nově nabyté dovednosti odkládat až na konec konfliktu, když si tím nyní můžete vydělat mnohem více peněz než v právní oblasti? Někteří hacktivisté, kteří se dotkli světa kyberzločinu, mu možná přijdou na chuť. Dříve nebo později se *"obrátí na temnou stranu "* – ať už jsou to kybernetické žoldáky nebo kyberzločinci. To se děje během všech konfliktů. Je jasné, že tomu tak bude i tentokrát.

„Všichni doufáme, že konflikt na Ukrajině brzy skončí. Z hlediska bezpečnosti však není důvod vydechovat. Naopak nárůst počtu kyberzločinců situaci pravděpodobně dále zhorší. Firmy a úřady by proto varování Federálního úřadu pro bezpečnost informací měly brát vážně a nespojovat je pouze se současnou politickou situací. Musí být schopni rychle podniknout protiopatření," poznamenává Werner v článku pro Der Tagesspiegel.

INFOKURÝR

Sdílet: