I “Vulkan Files” e la cyberwar di Putin

L’inchiesta “Vulkan Files” svela come la società russa Vulkan, che si occupa di sviluppo software e sicurezza informatica, lavori per i servizi segreti russi realizzando armi informatiche e fornendo servizi all’intelligence russa.

I documenti, che fanno riferimento al periodo che va dal 2016 al 2021, provengono da un informatore anonimo probabilmente interno alla NTC Vulkan che mosso dal disappunto per il cyber-conflitto invia al quotidiano tedesco Süddeutsche Zeitung circa 5.000 pagine dopo l’invasione Russa dell’Ucraina.

> *“People should know the dangers of this. Because of the events in Ukraine, I decided to make this information public. The company is doing bad things and the Russian government is cowardly and wrong. I am angry about the invasion of Ukraine and the terrible things that are happening there. I hope you can use this information to show what is happening behind closed doors.”*

Virgolettato riportato dal The Guardian, che insieme ad altri media internazionali indagano sul consistente fascicolo contenente documenti interni dove si raccontano gli strumenti messi a disposizione del Servizio di sicurezza federale russo (FSB), le sue forze armate (GOU e GRU) e il Servizio di intelligence estero (SVR) da parte della società Vulkan e apparentemente utilizzati in diverse operazioni informatiche di grande rilievo, come le interferenze nelle elezioni presidenziali degli Stati Uniti del 2016 e il cyber spionaggio.

Il 30 marzo 2023 vengono diffusi i primi dettagli dell’indagine, anche se un giudizio definitivo sulla veridicità rimane difficile da sostenere, i file appaiono

autentici a molteplici agenzie di intelligence; essi sono composti da progetti ben strutturati, comunicazioni email, dettagli di contratti e relativi budget.

Pur non essendo ancora confermato l'utilizzo degli strumenti realizzati da Vulkan in contesti reali, si indaga su possibili connessioni con gli attacchi informatici perpetrati da gruppi di cyber criminali risalenti alla Russia quali Sandworm, ritenuto responsabile di cyber attacchi su scala globale come il lancio del malware NotPetya, il blackout che per ben due volte ha paralizzato l'Ucraina e l'interruzione delle Olimpiadi in Corea del Sud. Le tecnologie messe a punto dalla Vulcan appaiono in grado di colpire infrastrutture critiche come le linee elettriche, trasporto ferroviario, marittimo e aereo.



Figure 1: Assessment of capabilities documented in NTC Vulkan aligned with broader strategic goals of Russian intelligence services
https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

Dai dati analizzati emerge la preferenza di target fortemente sensibili, quali le infrastrutture critiche e sistemi industriali, prediligendo l'indirizzamento di operazioni offensive verso obiettivi OT attraverso attacchi IT/OT. All'interno dei documenti si rintracciano i dettagli relativi a tre progetti in particolare: Scan – strumento che scansiona Internet alla ricerca di vulnerabilità da utilizzare in futuri attacchi informatici; Amesit – un framework per la sorveglianza e il controllo di Internet nelle regioni sotto il comando della Russia che consente anche la disinformazione tramite falsi profili di social media – e Krystal-2B – programma di formazione per operatori informatici sui metodi necessari per abbattere le infrastrutture ferroviarie, aeree e marittime.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/i-vulkan-files-e-la-cyberwar-di-putin/