Domínios fraudulentos procuram aproveitar falha da CrowdStrike

itsecurity.pt/news/threats/dominios-fraudulentos-procuram-aproveitar-falha-da-crowdstrike

Nos últimos dias, desde a **falha da CrowdStrike** na última sexta-feira (19 de julho), foram encontrados **67 domínios fraudulentos** associados à falha em questão.

A **VisionWare Intelligence Threat Center** alerta para o perigo iminente de "*novas campanhas de phishing e de uma nova onda de ciberataques resultantes deste incidente*".

De acordo com afirmações da própria CrowdStrike, e citada pela VisionWare, terá sido criada uma oportunidade para os cibercriminosos aproveitarem o momento, uma vez que a fragilidade dos sistemas afetados ainda permanece.

A falha da CrowdStrike está a ser aproveitada por cibercriminosos para tirar vantagens económicas, visto que já se assiste a esquemas fraudulentos através de falsas atualizações de ficheiros com vírus.

Assim, a VisionWare indica que "*é importante ser cada vez mais rigoroso com as regras e procedimentos a aplicar no controlo robusto aos fabricantes, tal como acontece nos processos de qualidade a outros fabricantes*".

Fonte da Equipa do VisionWare Threat Intelligence Center, centro de monitorização de ameaças à escala mundial da empresa portuguesa VisionWare, explicou em declarações à IT Security que "*estes dados só vêm a comprovar algo que todos nós receávamos, mas que já contávamos: uma escalada de manobras de engenharia social, explorando a instabilidade que as empresas visadas por este apagão têm sentido. Enfrentaremos, certamente, uma nova e intensa onda de ciberataques associados a esta ocorrência*".

"*São 8,5 milhões de computadores infetados, grande parte deles com o problema ainda por resolver. Será um processo lento e minucioso, que terá de envolver muito awareness e preparação, primeiramente, das empresas afetadas, mas também das autoridades competentes que terão de investigar criteriosamente e procurar respostas, pois os atacantes terão um período de tempo considerável para colocar em prática novos esquemas que permitam alcançar os seus objetivos*", diz a mesma fonte.

Os domínios fraudulentos já identificados são:

- crowdstrike-bsod[.]co
- crowdstrike-bsod[.]com
- crowdstrike-fix[.]zip
- crowdstrike-helpdesk[.]com
- crowdstrike-out[.]com
- crowdstrike[.]blue
- crowdstrike[.]bot
- crowdstrike[.]cam
- crowdstrike[.]ee
- crowdstrike[.]es
- crowdstrike[.]fail
- crowdstrike0day[.]com
- crowdstrikebluescreen[.]com

- crowdstrikebsod[.]co
- crowdstrikebsod[.]com
- crowdstrikebug[.]com
- crowdstrikeclaim[.]com
- crowdstrikeclaims[.]com
- crowdstrikeclassaction[.]com
- crowdstrikecure[.]com
- crowdstrikedoomsday[.]com
- crowdstrikedown[.]com
- crowdstrikedown[.]site
- crowdstrikefail[.]com
- crowdstrikefix[.]co
- crowdstrikefix[.]com
- crowdstrikefix[.]in
- crowdstrikefix[.]zip
- crowdstrikeglitch[.]com
- crowdstrikehelp[.]com
- crowdstrikelawsuit[.]com
- crowdstrikemedaddy[.]com
- crowdstrikeold[.]com
- crowdstrikeoops[.]com
- crowdstrikeoopsie[.]com
- crowdstrikeoopsies[.]com
- crowdstrikeout[.]com
- crowdstrikeoutage[.]com
- crowdstrikeoutage[.]info
- crowdstrikepatch[.]com
- crowdstrikeplatform[.]com
- crowdstrikeplatform[.]info
- crowdstrikerecovery[.]com
- crowdstrikereport[.]com
- crowdstrikesettlement[.]com
- crowdstrikesuporte[.]com
- crowdstrikesupport[.]info
- crowdstriketoken[.]com
- crowdstrikeupdate[.]com
- crowdstrikeyou[.]xyz
- crowdstrikezeroday[.]com
- fix-crowdstrike-apocalypse[.]com
- fix-crowdstrike-bsod[.]com
- fix-crowdstrike[.]com
- fixcrowdstrike[.]com
- fixmycrowdstrike[.]com
- fuckcrowdstrike[.]com
- howtofixcrowdstrikeissue[.]com
- iscrowdstrikedown[.]com
- iscrowdstrikefixed[.]com
- iscrowdstrikestilldown[.]com
- isitcrowdstrike[.]com
- microsoftcrowdstrike[.]com
- microsoftoutagescrowdstrike[.]com
- secure-crowdstrike[.]com
- suportecrowdstrike[.]com
- whatiscrowdstrike[.]com