

Forum:[Hack Forums](#)

Thread: [Vector sitting duck](#)

Aurelius - August 2, 2024, 12:02 pm

New attack being discovered named "vector sitting duck" in honor of a bird that probably discovered it , the powerful attack vector exploits weaknesses in the DNS , wich is being exploited to stealthily hijack domains .

sitting ducks is easier to perform , more likely to succeed , and harder to detect than other well publicized domain hijacking attack vectors .

According to the reports Several things contribute to the attack's success , first they register the domain with one entity and then give its management to another , its basically snatching an unused web address from under the physical noses of its owners .

Researchers say that they found millions of addresses susceptible to this problem, with thousands already being used for phishing , some of them belonged to big brands that kept an unused address until scammers hijacked it for good .

What are your thoughts on this attack ?

Eran - August 2, 2024, 12:50 pm

I thought this thread was about [Vector](#) and [flyingduck](#) when I first read the title lol

EDIT: nvm I confused [sector](#) with the guy above, I'm sleep deprived smh

flyingduck - August 2, 2024, 1:41 pm

THIS IS OUTRAGOUS! they use my good name for their shit :(now my plan to become the king of the world is canceled :(

istg if i find out that this was created by a user on here ... :@

Mr_Kh4os - August 2, 2024, 2:17 pm

(Aug 2, 2024 12:02 PM)BlackThoughts Wrote: [\[CITE\]](#) New attack being discovered named "vector sitting duck" in honor of a bird that probably discovered it , the powerful attack vector exploits weaknesses in the DNS , wich is being exploited to stealthily hijack domains .

sitting ducks is easier to perform , more likely to succeed , and harder to detect than other well publicized domain hijacking attack vectors .

According to the reports Several things contribute to the attack's success , first they register the domain with one entity and then give its management to another , its basically snatching an unused web address from under the physical noses of its owners .

Researchers say that they found millions of addresses susceptible to this problem, with thousands already being used for phishing , some of them belonged to big brands that kept an unused address until scammers hijacked it for good .

What are your thoughts on this attack ?

The insane part about this is we have known publicly at least since 2016 and there has been nothing really done about it. We talked about this very thing in class last Tuesday, literally anyone can do this too ? no software involved just a configuration issue that they don't seem to want to fix once they get the account you could sell traffic place ads anything. The context/why he brings it up as one of the examples to never depend on others work and raw knowledge over tools.

Thanks for the share!

