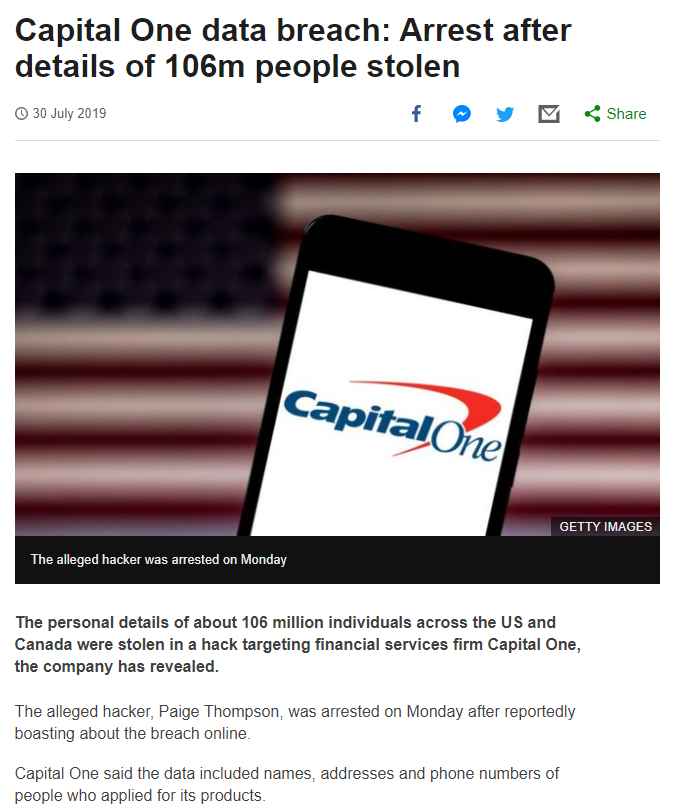


Մեգաքարտ (Megacart) խումբը EXIF ​​տվյալների մեջ թաքցնում է չարամիտ ծրագրերը

Մեգաքարտ (Խումբ 9)–համակարգչում քարտի սքիմերի (skimmer) ծածկագիր թաքցնելը այն մարտավարությունը չէ, որն օգտագործում է սպառնալիքների տերը: Սովորաբար, այս չարամիտ ծրագիրը տեղադրվում է կոմպրոմատային կայքի մեջ՝ փոխելով առկա JavaScript կոդը կամ անմիջապես բեռնելով հեռավոր սկրիպտ (script), սակայն նոր հարձակման մեջ Malwarebytes-ի հետազոտողները հայտնաբերել են, որ այս վնասակար JavaScript կոդը թաքնված է favicon պատկերի EXIF (փոխանակելի պատկերի ֆայլի ձևաչափ) տվյալների մեջ՝ հայտնաբերումից խուսափելու համար: Հարձակումը նկատվել է WordPRess-հիմքով կայքի վրա և օգտագործելով WooCommerce ներդիրը: Կոդը թաքցնելը պատկերի վերնագրերի մեջ, ինչպես արվել էր հարձակման ժամանակ, նոր տակտիկա չէ, բայց առաջին անգամն էր Malwarebytes ականատես էր եղել, որ չարաշահումը օգտագործվել էր կրեդիտ քարտի սքիմերի համար: Այս պարագայում սպառնալիքի տիրոջը հաջողվել է ջարդել կայքը և ավելացնել հասարակ սկրիպտ, որը մտնցրել էր հեռավոր favicon պատկերի մեջ cddn[.]site/favicon.ico-ից, փոքրիկ փոփոխություն է, որը հավանաբար կասկածելի չէր թվար ջարդված կայքի կոդի փոփոխությունները ուսումնասիրելուց: Անմիջապես հենց պատկերը բեռնվում էր կայք, ցանկացած կրեդիտ քարտի տվյալները այդ էջ մուտքագրված արտատպվում էին և ուղարկվում էին սպառնալիքի տիրոջը:



Կապիտալ մեկ (Capital one) տվյալի խախտում. Ձերբակալում 106 միլիոն մարդկանց գողացված տվյալների մանրամասնություններից հետո

**Մոտավորապես 106 միլիոն մարդկանց անձնական տվյալներ Ամերիկայով և Կանադայով մեկ գողացվել էին հակերության մեջ՝ թիրախավորած Capital one կազմակերպության ֆինանսական ծառայություններին, կազմակերպությունը բացահայտել է:**

Ենթադրյալ հակեր Փեյջ Թոմսոնը (Paige Thompson) ձերբակալվել է երկուշաբթի օրը՝ բացահայտ կերպով պարծենալով առցանց խախտման մասին:

Ըստ Capital one-ի տեղեկությունների՝ տվյալները ներառել են իր ապրանքների համար դիմած անձանց անուններ, հասցեներ և հեռախոսահամարներ:



Բաց աղբյուրի մատակարարման շղթան ավելացնում է 430% հարձակումներ

Ֆիլ Մունքաստր

Էլ.փոստ. phil Follow@philmuncaster

Անվտանգության մասնագետները նախազգուշացնում են ուղիղ բաց աղբյուրի բաղադրիչներին թիրախավորող 430 տոկոս տարեկան հարձակումների աճի մասին, որպեսզի գաղտնի վնասեն առանցքային ծրագրակազմի մատակարարման շղթան:

2019թ.-ի հուլիս և 2020թ.-ի մայիս ամիսների ընթացքում գրանցվել են 929 հարձակումներ՝ ըստ *առանցքային ծրագրակազմի մատակարարման շղթայի իրավիճակի* մասին Սոնաթայփի (Sonatype) տարեկան զեկույցի: Այս ուսումնասիրությունը հիմնված է 24,000 բաց աղբյուրի ծրագրային վերլուծության և 15,000 զարգացման կազմակերպությունների, ինչպես նաև 5600 ծրագրակազմի մշակողների հետ հարցազրույցների վրա:

Չարամիտ դերակատարների կողմից բաց աղբյուրի բաղադրիչներին թիրախավորելը անհանգստացնող է ՝ առևտրի ժամանակը (time-to market) արագացնելու DovOps թիմում իրենց հայտնիության համար: