禪

188 [illegible]

[illegible]

Parkeertijd eindigt op
DAG
UUR
288 10:36
14/10/16 1,50 € 734
Parkeertijd eindigt op
DAG
UUR
288 11:52
Parkeertijd eindigt op
DAG
UUR
287 18:48
13/10/16 0,00 € 114
PRIJS
STAD GENT
Leesbaar achter de voorruit te plaatsen

[illegible]

مطلب پیشنهادی

بیگانه‌ای پرسه میزند شماره 187

حمله_کرم به چراغهای هوشمند شهری

هکرها میتوانند برنامه‌ای بنویسند که قادر باشد رسیدهای پارکینگ را کپی /رونویسی کند . این برنامه بهطور خودکار قادر است مکان کاربر را شناسایی کرده و فهرستی از پارکینگهایی که در نزدیکی او قرار دارند را نشان دهد . در ادامه میتواند تصویری از یک رسید پارکینگ معتبر را ارائه دهد . این شیوه هک عمدتاً موردپسند دانشآموزان و جوانان است، بهدلیل اینکه زمان آزاد بیشتری در اختیار دارند . در بخش دیگری از این منطقه سامانه‌ای قرار دارد که بر مبنای پیام کوتاه کار کرده و قادر به توزیع بلیطهای یک ساعته برای سامانههای حمل و نقل است. برعکس رسیدهای پارکینگ این بلیطهای مبتنی بر پیام کوتاه یک شناسه منحصر بهفرد دارند و بهراحتی امکان رونویسی آنها وجود ندارد . با این حال هکرها میتوانند یک برنامه وبمحور را طراحی کرده و از این برنامه بهمنظور به اشتراکگذاری بلیطها استفاده کنند . بهطور مثال، کاربری بلیطی را خریداری کند و 20 دقیقه از سامانههای حمل و نقل استفاده کند، در این حالت هنوز هم 40 دقیقه زمان برای استفاده از این بلیط وجود دارد . اما با استفاده از یک برنامه هکری این امکان وجود دارد که این 40 دقیقه را میان افراد مختلف به اشتراک قرار داد .

در پایان هر ماه، مشترکان این برنامه صورتحسابی را دریافت کرده و از طریق بیتکوین وجه موردنظر را به حساب هکر واریز میکنند . این سامانه بهراحتی و در عین حال بهشیوهای کاملا تمیز به افراد مختلف اجازه میدهد از سامانههای حملونقل با کمترین قیمت استفاده کنند . حتی فرآیند بازیافت بطریها در فروشگاههای مواد غذایی نیز در تیرراس هکرها قرار دارند . زمانی که یک مشتری نوشیدنی خود را تمام کرد، بطری را در قفسه مربوطه قرار میدهد و با اسکن بارکد حک شده روی بطری وجهی را از بابت فرآیند بازیافت بطری دریافت میکند . مقدار بازخریدهای نقدی برای بطریها متفاوت است . اما هکرها به این حقیقت آگاه شدهاند که میان مبلغ بازگردانده شده و بارکد هیچگونه همبستگی وجود ندارد . در نتیجه با رونویسی یکی از بارکدهایی که مبلغ بالایی را دارند یک هکر میتواند مبلغ بازخرید بیشتری دریافت کند . مشکل فوق به این دلیل بهوجود آمده است که مسئولان این سامانهها را بهشکلی طراحی نکردهاند تا اختلاف قیمت را تشخیص دهد. در نتیجه یک هکر قادر است با چند بار تکرار این فرآیند پول خوبی بهدست آورد . جالب آنکه دیدگاه افراد ساکن در شهرهای هوشمند اروپایی با یکدیگر تفاوت دارد . بهطور مثال یک شهروند بلژیکی عنوان کرده است که این ترفندها یک کلاهبرداری ساده هستند .

در حالی که شهروند دیگری گفته است : «اینگونه فعالیتها بازی کردن با سامانههای شهری است . زمانی که فردی در یک شهر زندگی میکند، اگر تخصص و توانایی مربوطه را در اختیار داشته باشد، قادر است از مزایای این چنین ترفندهایی بهر شکلی که میتواند استفاده کند ». همین موضوع باعث شده است تا کارشناسان امنیتی به برنامهریزان شهرهای هوشمند هشدار دهند : «مردم قادر هستند بهخوبی با سامانههای هوشمند بازی کنند . افراد بسیاری وجود دارند که به راحتی میتوانند قوانین و روند فعالیت یک سامانه را شناسایی کرده و بهراحتی بهآن نفوذ کنند . هر چند برنامهریزان شهری در شهرهای هوشمند با کلاهبرداری در مقیاس کم کنار آمدهاند اما زمانی که سامانههای حساس همچون شبکه برق، چراغهای راهنمایی و سامانههای کنترل دسترسی در معرض تهدید هکرها قرار گیرند بدون شک به سطح بالایی از امنیت و نظارت نیاز خواهند داشت ».

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
20:38 - 30/10/1395

برچسب:
شهر_هوشمند - حمله_هکری

□□□□□ منبع: https://www.shabakeh-mag.com/security/6432