به نام خدا

آیا می دانید هکرها می توانند به دوربین دوربین مدار بسته شما دسترسی پیدا کنند و از آن برای راه اندازی استفاده کنند.ویا کلا آنها را بسوزانند.

ممکن است شما یک سیستم دوربین مداربسته برای یک مشتری نصب میکنید،که این سیستمی که نصب میکنید یکی از این موارد است:یا دوربینipیا دوربینبه دستگاه دی وی آرhdیادوربینipبه دستگاهnvr.

وحالا برای انتقال تصویر از تکنولوژیp2pاستفاده میکنید.برای اینکه مشتری از طریق اینترنت بتواندتصاویر مکان خودرا مشاهده کند.

این نمونه انتقال تصویرp2p بسیار آسان است وبه راحتی میتوان تصاویر دوربین های مداربسته را برروی اینترنت قرار داد.

خوب،دراینترنت بحث های زیادی برای انتقال تصویریک دستگاه dvrوجود دارد که بتوان دستگاه را برروی اینترنت فعال کرد وتصاوی ررا از راه دور مشاهده کرد.

خیلی از دوستان میگویند"من نیاز به یادگیری هرگونه تنظیمات پیشرفته درمورد مودم وای فای ویا دستگاهای دوربین های مداربسته ویا چیزها کلیشه ای ندارم،چون وقتی که تولید کنندگان دوربین های مداربسته یک راه آسان برای انتقال تصویر گذاشتند که همانp2pمیباشد.فقط با یکی دوتا کلیک میتوان به سرعت انتقال تصویر انجام داد.

حقیقت این است که دستگاه های زیادی در اینترنت بدون هیچ مشکلی با مسائل امنیتی متصل شده اند. مشتریان هیچ ایده ای ندارند که چطور از دستگاهایشان محافظت کنندونصب کنندگان دوربین مداربسته معتقد هستندکه روشp2pآسانترین روش در دوربین های مداربسته برای انتقال تصویر میباشد .

اما حدس بزن چه اتفاقی می افتد وقتی دوربین شما محافظت نمی شود وامنیت آنها کاملا پایین می آید؟به راحتی میتوان آن را هک کرد ودر هرزمان هکرها به تصاویر دسترسی پیدا خواهند کرد.

در این مقاله، من در مورد یک مشکل جدی به نام تروجان (ویروسهای اینترنتی)صحبت خواهم کرد، یک نوع ویروس که به دستگاهIP شما دسترسی پیدا می کند و می تواند توسط هکرها که از راه دور به دستگاها برای حمله ویا به سرورهای دیگر در اینترنت استفاده کنند،

شرکت های که خدمات انتقال تصویر p2pرا میدهند،اگر دریک مکانی که دوربین مداربسته نصب کردید وبخواهید از طریق اینترنت انتقال تصویر بگیرید،تولید کننده دستگاهای دوربین مداربسته باید این خدمات را اراعه دهند تا شما بتوانید انتقال تصویر بگیرید.یعنی اینکه وقتی شما انتقال تصویر میگیرید اول باید دستگاه مثلاdvrبه شرکت سازنده وصل شود وبعدبتوان انتقال تصویر گرفت.به نظر من به این حالت است که؛اول تصاویر برای شرکت سازنده فرستاده میشود وبعد شرکت تصاویر را برای ما ارسال میکند.

پیشنهادمیکنم که این مقاله را حتما مطالعه کنید:آموزش انتقال تصویردوربین های مداربسته بدون نیاز به اینترنت

دراینجا میخواهم در مورد مفهومی به نامDDoSاستفاده کنم که بدانید این مفهوم چیست وچه کارای در دوربین های مداربسته دارد

DDoS چیست؟؟

DDoS مخفف Denial of Service است یعنی اینکه سرازیر کردن تقاضای زیاد به یک سروراست.یعنی اینکه چندین دستگاه به طور همزمان به یک سرور وصل شود وآن سرور نتواند پاسخ گوی آنها باشد مجبور آنها را رد کند،یعنی همزمان نمیتواند به تمام درخواست ها پاسخ دهد وسپس شروع به رد کردن سرویسها برای انتقال تصویر میکند.
مانند یک دسته از افرادی که به بیمارستان نیازمندند و دیده می شوند، اما زمانیکه تمام پزشکان از آنها مراقبت می کنند، به این ترتیب کسانی که دوباره مراجعه میکنند واقعا نیاز به خدمات دارند نمی توانند آنها را قبول کنند.

رابطه بین دوربین های مداربسته و حملهDDoS چیست؟

هنگامی که یک ویروس یا هکر به یک دوربینIP، DVR یا NVR وارد می شود، می توان از این دستگاه ها برای راه اندازی یک حمله هماهنگ شده به یک هدف در اینترنت استفاده کرد. تصور کنیدDVR شما بخشی از یک سیستم است که درخواست اتصال به سرور ها را دارد وسرور پاسخگو نیست به همین خاطر دستگاه شما دراختیار حملهddosقرار میگیرد

بنابراین باید مراقب باشیم که سیستم مداربسته مورد حمله قرار نگیرد

بهتر است که وقتی انتقال تصویر میگیرید پسورد دستگاهdvr؛nvrویا دوربینipرا عوض کنید واز پسوردهای مشکل استفاده کنید تا دستگاه توسط هکرها هک نشود.که البته به نظر من برای انتقال تصویربه جایp2p بهتر است ازipثابت استفاده کنید.

درجدول زیر نمونه ای از کلمات عبورپیشفرز دستگاهای سازنده دوربین های مداربسته آورده شده،که میتوانید با رمز عبور دیفالت انواع دستگاهها آشنا شوید.::

سازندگان سیستم مداربسته	پسورد/یوزرنیم
ACTi IP Camera	admin/123456
ANKO Products DVR	root/anko
Axis IP Camera, et. al	root/pass
Dahua Camera	root/vizxv
Dahua DVR	root/888888
Dahua DVR	root/666666
Dahua IP Camera	root/7ujMko0vizxv
Dahua IP Camera	root/7ujMko0admin
Dahua IP Camera	666666/666666
Dreambox TV receiver	root/dreambox
EV ZLX Two-way Speaker?	root/zlxx
Guangzhou Juan Optical	root/juantech
H.264 - Chinese DVR	root/xc3511
HiSilicon IP Camera	root/hi3518
HiSilicon IP Camera	root/klv123
HiSilicon IP Camera	root/klv1234
HiSilicon IP Camera	root/jvbzd
IPX-DDK Network Camera	root/admin
IQinVision Cameras, et. al	root/system
Mobotix Network Camera	admin/meinsm
Packet8 VOIP Phone, et. al	root/54321
Panasonic Printer	root/00000000
RealTek Routers	root/realtek
Samsung IP Camera	admin/1111111
Shenzhen Anran Security Camera	root/xmhdipc
SMC Routers	admin/smcadmin
Toshiba Network Camera	root/ikwb
Ubiquiti AirOS Router	ubnt/ubnt
VideoIQ	supervisor/supervisor
Vivotek IP Camera	root/<none>
Xerox printers, et. al	admin/1111
ZTE Router	root/Zte521

abarelectronic.com

بنابراین ما باید مراقب باشیم که بخشی از یک سیستم حمله نباشیم و ما

می توانیم با تغییر گذرواژه پیش فرض دستگاه واستفاده ازipثابت از هک شدن دستگاه خود جلوگیری کنیم.

این فیلم آموزشی راحتما ببینید:**تنظیمات مودم برای انتقال تصویر دوربین های مداربسته**

انواع فیلم های آموزشی دوربین های مداربسته را هم دانلود نمایید.

http://abarelectronic.com/downloads