Forum:Hack Forums

Thread: Wireless town CCTV system

zerocool - *December 6, 2015, 2:21 am*

My local town has just upgraded it's cctv system, from what i can see its a wireless system like the image below.
Spoiler (Click to View)
[img]http://www.cordless4u.com/images/MultiPoiintWirelessCamerasetup.jpg[/img]

Has any one ever tried to get on this type of system, any one have any ideas i know it's most likely a bad idea but still fun at the same time.

Mad76e - *December 6, 2015, 4:00 am*

Yeah.. Trough shodan not from the wireless side. I know that you can defend yourself, so in this case its just fun. The hardest part is to get access to the main router.

Some thoughts

IF some camera is out of order, use that macadress to get access. Open up a mac-address in The whitelist, so you dont have to use one of the cameras to get access

IF you break the. Encryption it may be possible to tap the feed

Also theres a bunch of vulns in many of the newest cameras out there, its also a way in

zerocool - *December 6, 2015, 4:10 am*

(Dec 6, 2015 05:00 AM)mad76e™ Wrote: *[CITE]* Yeah.. Trough shodan not from the wireless side. I know that you can defend yourself, so in this case its just fun. The hardest part is to get access to the main router.

Some thoughts

IF some camera is out of order, use that macadress to get access. Open up a mac-address in The whitelist, so you dont have to use one of the cameras to get access

IF you break the. Encryption it may be possible to tap the feed

Also theres a bunch of vulns in many of the newest cameras out there, its also a way in
I have tried shodan but sadly wasn't there, i'm sure its just a local network all shared via point to point, gunna try an get some pics see if i can tell what models they are.
Got a feeling it's shared via these, not the same but defo that logo
https://i.imgur.com/DVgpdnm.png

Feanor - *December 6, 2015, 4:20 am*

I've subbed to the thread are you going to keep updating?

zerocool - *December 7, 2015, 1:00 am*

(Dec 6, 2015 05:20 AM)Feanor Wrote: *[CITE]* I've subbed to the thread are you going to keep updating?

Going to try an sneak some picture's today of the setup see if any one know's the equipment.

Frosteh - *December 7, 2015, 1:34 am*

edit

Sorry I wrote a post without reading all your responses, you've already identified the units, so it looks like these then? https://www.ubnt.com/airmax/nanostationm/

I wouldn't know the first thing about actually getting onto the network, it'll be encrypted which means you'll need to join the network first, looking at some of the PDFs for the devices it looks like the security can use WPA2-AES, WEP or even none!!! (fucking facepalm). Looks like they're using the 5Ghz band. So it looks like these cheaper ones are actually just slightly more fancy network devices with directional antennas and PoE, so I'd guess that traditional network attack tools for Wifi will work.

Assuming they're not being dumb and using an OPN/WEP network, you'll want to look at seeing if you can force a de-auth with aireplay and monitor for a 4 way handshake, that'll be a bit tougher than normal because you need messages from both the AP and the client which will probably require a directional antenna for your wifi. Once you have a 4 way handshake you can try and crack that offline with something like ocl-hashcat with some large password dictionaries.

I guess there's all sorts of ways to potentially attack these things, the simplest might be the riskiest which is to actually get physical access to one, they have basic web interfaces which have default username/passwords (ubnt/ubnt) which I'd expect they'd change but worth trying, they're probably open to brute force otherwise. It doesn't look like they have any physical security covering the LAN ports just a port release button around the back.

Attacking the actual IP cameras is another thing entirely once you're on the wireless network or you can tap the ethernet, I guess find out the make the of the camera and look for exploits, one thing to note is that these things are typically not at all secure despite their importance, recent defcon video had a guy find 3 major brands recently were rootable because of dumb security practices with web interfaces etc. If they're not SSL and use plaintext transmition then you can just sniff the network for people logging on.

Mad76e - *December 7, 2015, 3:35 am*

(Dec 6, 2015 05:10 AM)z3roc00l Wrote: *[CITE]* I have tried shodan but sadly wasn't there, i'm sure its just a local network all shared via point to point, gunna try an get some pics see if i can tell what models they are.
Got a feeling it's shared via these, not the same but defo that logo
https://i.imgur.com/DVgpdnm.png
that is without doubt the Ubiquiti logo (if you didn't figure it out by now)
[img]http://www.nv-networks.com/media/wysiwyg/ubnt_logo_basic_flat_color.jpg[/img]

Ubiquiti is told to be the "Rolls-Royce" in the wireless network, especially long range. It has both antennas, access points and wifi-sticks, some of them injection capable, but sadly they are expensive as fuck. The Routers/AP:s is a wet dream for any nerd with a lot of settings and tweaks to help the owner to get maximal performance. only thing stopping me from throwing mt alfas

zerocool - *December 7, 2015, 4:12 am*

(Dec 7, 2015 04:35 AM)mad76e™ Wrote: *[CITE]* that is without doubt the Ubiquiti logo (if you didn't figure it out by now)
[img]-snip-[/img]

Ubiquiti is told to be the "Rolls-Royce" in the wireless network, especially long range. It has both

antennas, access points and wifi-sticks, some of them injection capable, but sadly they are expensive as fuck. The Routers/AP:s is a wet dream for any nerd with a lot of settings and tweaks to help the owner to get maximal performance. only thing stopping me from throwing mt alfas
Yes i did notice that was from Ubiquiti, i found out that the whole system cost just under £75,000 that included moving the local police to digital radio's.
Most of it was spent on the cctv upgrade for 18 camera's.

Green Goblin - *December 8, 2015, 1:12 pm*
This reminds me of watch dogs :p

soxrok2212 - *December 8, 2015, 2:10 pm*
(Dec 7, 2015 04:35 AM)mad76e™ Wrote: *[CITE]* The Routers/AP:s is a wet dream for any nerd with a lot of settings and tweaks to help the owner to get maximal performance.
That gave me a good laugh, and it is so true! ?
Yeah, ubiquity products are really nice pieces of hardware.

ST34M - *December 8, 2015, 2:40 pm*
(Dec 6, 2015 05:00 AM)mad76e™ Wrote: *[CITE]* Yeah.. Trough shodan not from the wireless side. I know that you can defend yourself, so in this case its just fun. The hardest part is to get access to the main router.

Some thoughts

IF some camera is out of order, use that macadress to get access. Open up a mac-address in The whitelist, so you dont have to use one of the cameras to get access

IF you break the. Encryption it may be possible to tap the feed

Also theres a bunch of vulns in many of the newest cameras out there, its also a way inThis why they call you the 'WiFi' guy.