

Our Time in a Product Review Cabal

And the **malware** and **bugs** that came with it

Adam Schaal
@clevernyyyy

Matt Virus
@themattvirus



Humans-in-the-loop



Adam Schaal



HARDWARE SKILLS



SOFTWARE SKILLS

- Head of AWS SHINE
- Homelab Enthusiast
- Community Involvement
 - Kernelcon Board Member and Founder
 - DEF CON 402 Board Member
 - Loco Moco Sec Organizer
 - O.MG Cable Alumni



Matt Virus



HARDWARE SKILLS



SOFTWARE SKILLS

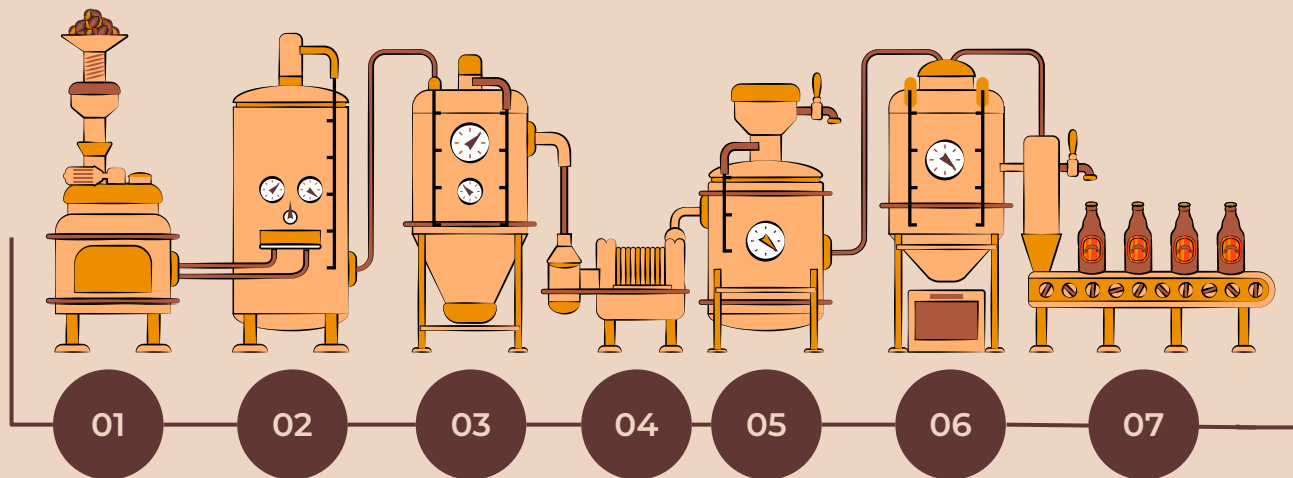
- IoT engineer at Cisco (17+ years)
- Part-time farmer
- Hardware junkie
- Former DoD (US) forensics and malware analyst
- Founder of hackspace.io
- Kernelcon Hardware Hacking Chair

Boilerplate Disclaimer

- All of this work was done for **research purposes only**.
- Nothing we discuss today is representative of our employer's views, opinions, or research.
- We ensured that every review, photo, and video were immediately taken down and reported.
- Platform agnostic. This affects **all online retailers**, not particular platforms.
- We strive to be an **ethical cabal**.
- Lastly, we're definitely here for the security and community despite what our slides may look like.



Today's Brewing Process



01	Milling & Mashing	How we got started and how we formed the cabal
02	Boiling	Scaling our cabal and noticing odd patterns
03	Cooling & Fermentation	Deep dive into some of our free products

04	Centrifuge	Scaling our work with AI
05	Carbonation	Cautionary tales
06	Bright Tank	How to purchase online safely
07	Bottling	Wrap up, Santé!

01

Milling & Mashing

How'd we end up with a closet full of gear?



2020 COVID-19 Pandemic

We're not just here for the beer.



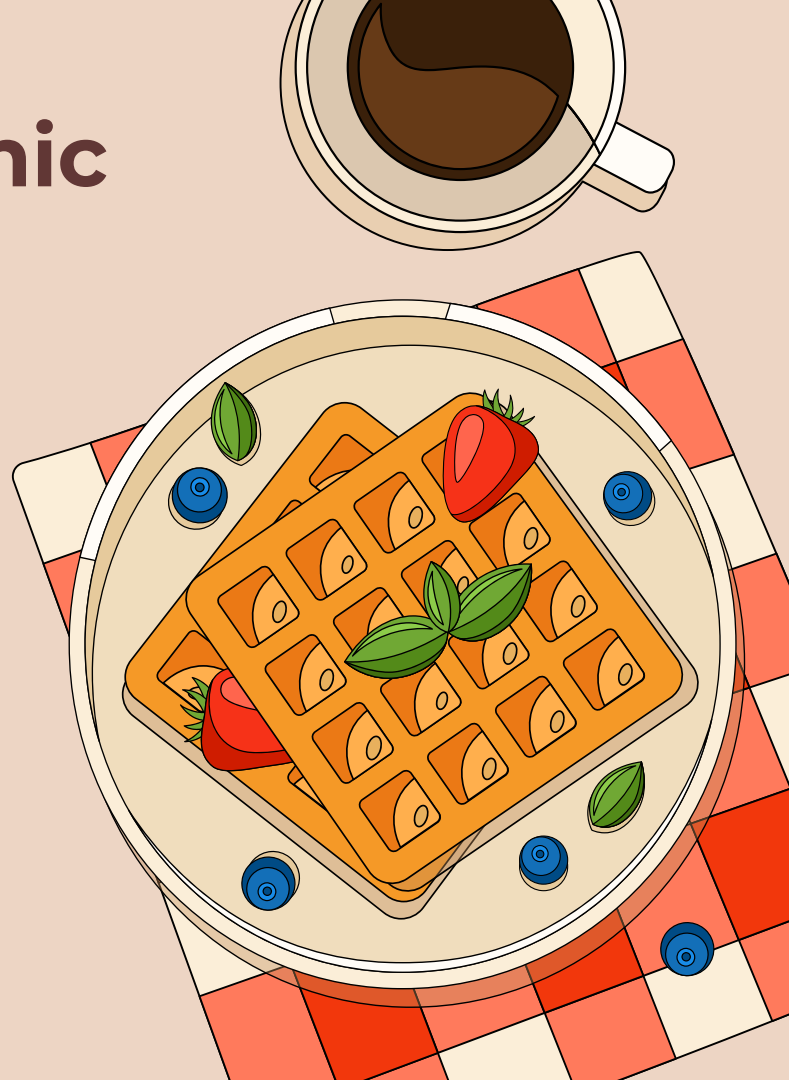
Masks



Streaming Media



Online Shopping

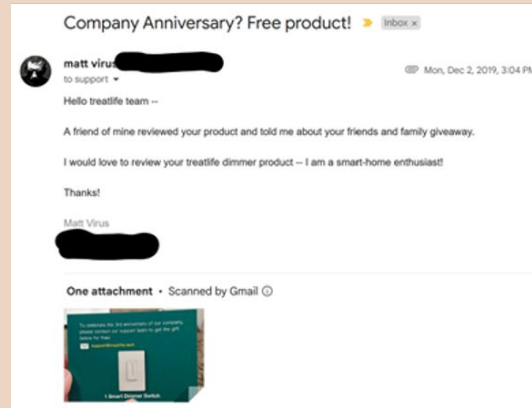


Our journey started with a postcard...

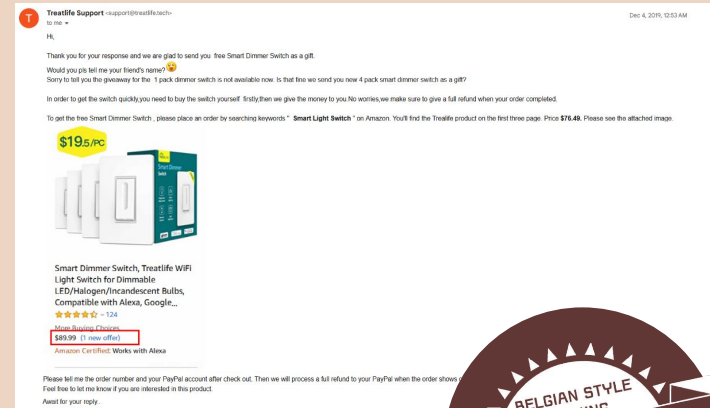
1



2



3



4

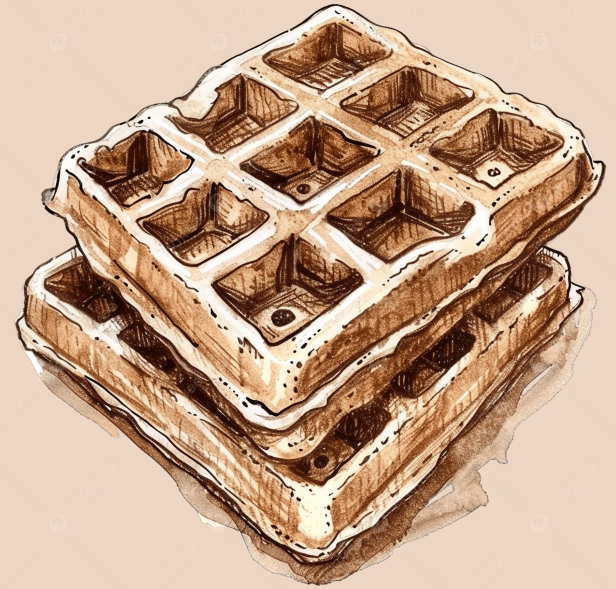
Profit!



02

Boiling

How can we make this concept scale?



But what if we wanted two?



We needed to think like a hacker...

- What if we interacted from different email addresses?
- Would they notice?



But what if we wanted two?



They did not!

We needed to think like a hacker...

- What if we interacted from different email addresses?
- Would they notice?



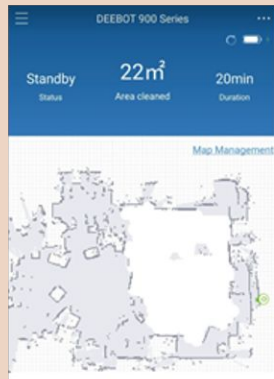
It scaled...



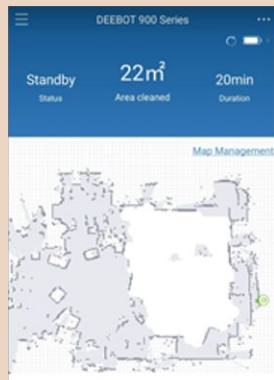
ESCAM PVR008
Power: 5V
Lens: 3.6mm
User Name: admin
NO Password
Made in China



And scaled...



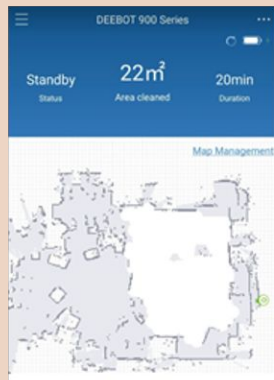
And scaled...



And scaled...



ESCAM PVR008
Power: 5V
Lens: 3.6mm
User Name: admin
NO Password
Made in China



Jealous Friends



Friends were jealous of our cool loot...

SO WE SHARED!

By referring people to vendors, they suddenly starting receiving their own invites.

Some were official referrals, but with others, we just started modifying forwarded email body/headers/etc and replied directly.

We Soon Realized...

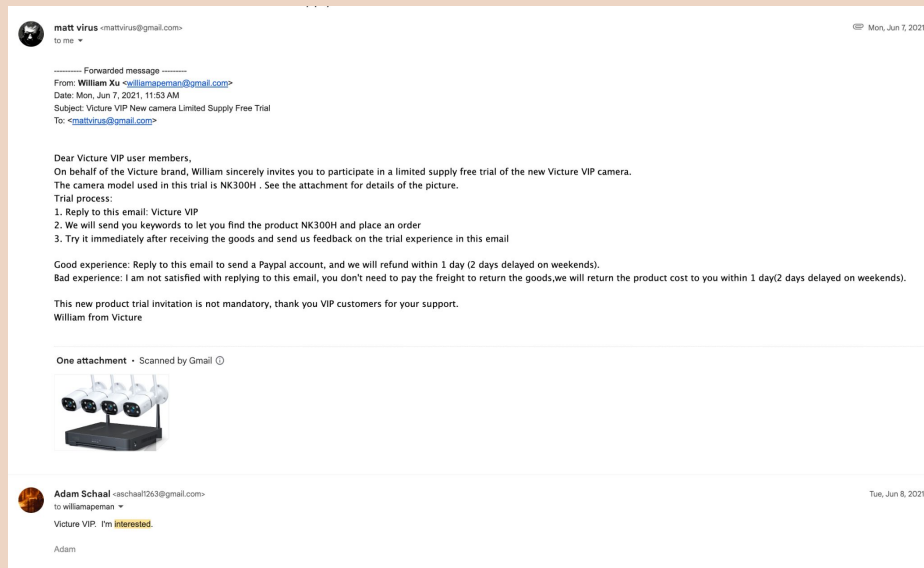
No one cared who responded.

Not only that, but they didn't seem to know who they sent the original messages to.

That means we could pass invites around.



Forming the Cabal



Whoa that really escalated

Inbox	Fwd: Free!!!!We invite you test new products-Webcam&Dual Band Wi-Fi Router&Wireless Video Doorbell&Dual Band Wi-Fi Router&Table Lamp - com\Victure-sc30\pr\TBK-075Y-00006?Item=9SIB3WTF...	11/15/21
Inbox	Fwd:Victure VIP New camera Limited Supply Free Trial -Victure VIP. I'm interested. Adam > > From: William Xu > Date: Mon, Jun 7, 2021, 11:53 AM > Subject:Victure	6/8/21
Inbox	Fwd: Hi friends,cover full pp fees , we need US US reviewer, need 5 star review , massage gun, baby monitor, dash cam and blood pressure monitors worth 300 USD ! ! - ----- Forwarded mess...	5/11/21
Inbox	Free WIFI Dash Cam for You! (Only US) - Susie fromVicture. So sorry for disturbing you and thank you very much for your reading this email. My colleague told me that	3/3/21
Inbox	Fwd: cnschaal@gmail.com - Lily fromVictureAre you interested in reviewing our products with a 100% full refund? If yes, you could join our promotion	2/1/21
Inbox	Fwd: Warm Greetings fromVicture!(Only US) - From:Victure Support Date: Tue, Dec 22, 2020, 9:51 PM Subject: Warm Greetings fromVicture!(Only US) To: Dear Customer	12/23/20
Inbox	Fwd: Warm Greetings fromVicture!(Only US) - From:Victure Support Date: Tue, Dec 22, 2020, 9:48 PM Subject: Warm Greetings fromVicture!(Only US) To: Dear Customer	12/23/20
Inbox	Fwd: cnschaal@gmail.com - with ourVicture products! 🧑🏻💻👉👉 Are you interested in reviewing our products with a 100% full refund? If yes, you could join	12/18/20
Inbox	Fwd: \$ 120 Smart Look Test Review Invitation fromVicture(USA) - Invitation fromVicture(USA) To: cnschaal Hi Friend, This is Lucy from the officialVicture Service Team. As you browsing	11/9/20
Inbox	Fwd: 4PCS Outdoor WiFi Secuirty Camera System for test! Worth \$190! - ----- Forwarded message ----- From: 752685779 <752685779@qq.com> Date: Wed, Oct 14,	10/16/20
Inbox	Greetings! Refund fromVicture! - Susie fromVicture Support Team. Many thanks for your precious time to read this letter. Could you please tell us if you remember	9/17/20
Inbox	Fwd: Kids camera need test - com\Victure-Rechargeable-Shockproof-Camcorder-Christmas!dp/B0822R3WF6/ref=sr_1_35?dchld=1&keywords	9/9/20
Inbox	Fwd: Be the First One to Test Our New Product - Victoria fromVicture. How is your day going? >>>> I have good news for you! Our company launches some new	8/29/20
Inbox	Fwd: Free Webcam for You - keyword: victure webcam (page 1 to 2 to search, >>> \$59.99) Please note to use this keyword not others to search	8/17/20
Inbox	Fwd: (Only US)Testing expensive camera and infrared Thermometer - That is so great,my friend,and may i ask do you have any friend need this?I just need many reviews,	8/16/20
Inbox	A Chance to Win Router - Victoria fromVicture. How is your day going? I have good news for you! Our company launches some new products and I want to	8/12/20
Inbox	A Chance to Win Router - Victoria fromVicture. How is your day going? I have good news for you! Our company launches some new products and I want to	8/12/20
Inbox	Fwd: A Chance to Win Router - Victoria fromVicture. Our company launches some new products and I would like to tell you that we have machines for giving	8/3/20
Inbox	Fwd: the step to find the product - YES, you can cancel the order, because the camera now no need a test at present I will have a good	8/2/20
Inbox	Fwd: A Chance to Win Router - Victoria fromVicture. Our company launches some new products and I would like to tell you that we have machines for giving	7/31/20
Inbox	Refund fromVicture - it's justVicture reviews. Adam On Wed, Jul 29, 2020 at 12:26 PM giveaways wrote: > Dear Customer, >> Have you	7/31/20
Inbox	Fwd: A special invitation for you! - From: victure Jessica Date: Sat, Jul 25, 2020, 7:46 AM Subject: A special invitation for you! To: Dear friend, Wish you all	7/25/20
Inbox	Fwd: Free Webcam for You^_^ - Lingling fromVicture.* So sorry for disturbing you and thank you very much for your reading this email. *My colleague told	7/24/20
Inbox	Fwd: a special activity for our loyal customer - 26 PM victure Jessica > wrote: >>> Great, thanks! >>> Adam Schaal 于2020年5月20日周三 上午11:13写道	5/26/20
Inbox	Fwd: Spend 2 minutes to get a Vitcure wifi camera/baby monitor. - PM Jolin Victure > wrote: >>> Have a nice day >>> Adam S 于2020年5月13日周三 上午11:15写道: >>>	5/18/20

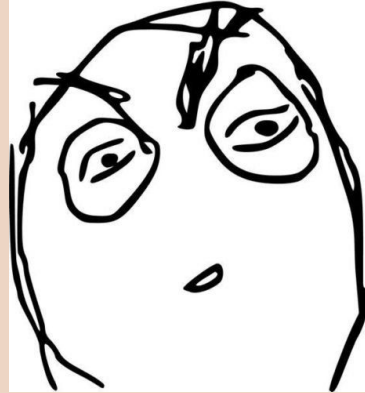
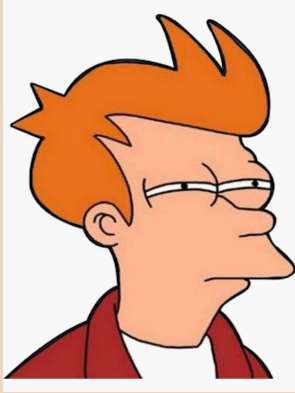
Whoa that really escalated

Inbox	Fwd: Free!!!!We invite you test new products-Webcam&Dual Band Wi-Fi Router	Inbox	Fwd: Review - ----- Forwarded message ----- From: 符典 Date: Mon, Mar 28, 2022, 3:56 AM Subject: Review To: ----- Forwarded message ----- From: Diana <2416273260@qq.com> Date: Thu, Oct 28, 2021, ----- Forwarded message ----- From: Diana <2416273260@qq.com> Date: Thu, Oct 28, 2021,	3/28/22
Inbox	Fwd: Free!!!!We invite you test new products-Webcam&Dual Band Wi-Fi Router	Inbox	Fwd: Free!!!!We invite you test new products-Portable DVD & Projector - ----- Forwarded message ----- From: Diana <2416273260@qq.com> Date: Thu, Oct 28, 2021,	10/28/21
Inbox	Fwd: Victure VIP New camera Limited Supply Free Trial - Victure VIP, I'm intere	Inbox	Fwd: 2.7k VideoKamera Testeinladung hinter dem APEMAN Fernglas (vergangenes Jahr) - hinter dem APEMAN Fernglas > (vergangenes Jahr) > > Hello, >> Yes, I enjoyed working with you and a...	8/6/21
Inbox	Fwd: Citibank has issued a Payout - PayPal APEMAN INTERNATIONAL CO.,LIMITED has sent you \$55.99 USD NOTE FROM APEMAN INTERNATIONAL CO.,LIMITED. [image	Inbox	Fwd: Citibank has issued a Payout - PayPal APEMAN INTERNATIONAL CO.,LIMITED has sent you \$55.99 USD NOTE FROM APEMAN INTERNATIONAL CO.,LIMITED. [image	6/8/21
Inbox	Fwd: Hi friends,cover full pp fees , we need US US reviewer, need 5 star review	Inbox	Fwd: Citibank has issued a Payout - PayPal APEMAN INTERNATIONAL CO.,LIMITED has sent you \$99.99 USD NOTE FROM APEMAN INTERNATIONAL CO.,LIMITED. [image	5/8/21
Inbox	Free WIFI Dash Cam for You! (Only US) - Susie from Victure , So sorry for distur	Inbox	Fwd: Hi friends,cover full pp fees , we need US US reviewer, need 5 star review , massage gun, baby monitor, dash cam and blood pressure monitors worth 300 USD ! I - and "Apeman Tour" App" ...	5/11/21
Inbox	Fwd: cnschaal@gmail.com - Lily from Victure Are you interested in reviewing	Inbox	FW: Sincere Greeting from Susan - us? APEMAN New Generation Ultra HD 1080P Front and Interior Dash Cam have been launching this week in US Amazon. As a gesture	5/8/21
Inbox	Fwd: Warm Greetings from Victure !(Only US) - From: Victure Support Date: Tul	Inbox	RE: Sincere Greeting from Susan - Sue from APEMAN . Do you still remember us? APEMAN New Generation Ultra HD 1080P Front and Interior Dash Cam have	5/8/21
Inbox	Fwd: Warm Greetings from Victure !(Only US) - From: Victure Support Date: Tul	Inbox	Fwd: P*ree binoculars from the Apeman brand - from the Apeman brand To: Dear friend, This is Aimee from the APEMAN customer center. Thank you very much for your support	5/5/21
Inbox	Fwd: cnschaal@gmail.com - with our Victure products! 🍕🍷 Are you intere	Inbox	Fwd: Direct Ship FREEBIES!!! - only for Apeman guys to receive a new product from APEMAN . All you need to do is to FILL OUT the form & JOINED our group. (	5/4/21
Inbox	Fwd: \$ 120 Smart Look Test Review Invitation from Victure (USA) - Invitation fr	Inbox	Fwd: RE: Sincere Greeting from Susan - Sue from APEMAN . Do you still remember us? APEMAN New Generation "Ultra HD 1080P Front and Interior Dash Cam" have been launching	4/30/21
Inbox	Fwd: 4PCS Outdoor WiFi Security Camera System for test! Worth \$190! - ----	Inbox	Fwd: RE: Sincere Greeting from Susan - Sue from APEMAN . Do you still remember us? APEMAN New Generation "Ultra HD 1080P Front and Interior Dash Cam" have been launching	4/26/21
Inbox	Greetings! Refund from Victure ! - Susie from Victure Support Team. Many thar	Inbox	Fwd: Free Camera for You from APEMAN ! - You from APEMAN To: Cnschaal Dear Customer, How are you? This is Susie from APEMAN Service Team. So sorry for disturbing	4/11/21
Inbox	Fwd: Kids camera need test - com Victure -Rechargeable-Shockproof-Camo	Inbox	Congratulation, You are chosen as a lucky one to get a free floor lamp - support of apeman brand before. Now we have a new product of floor lamp worths \$29.99 start to sell. We want to find 20 e...	3/30/21
Inbox	Fwd: Be the First One to Test Our New Product - Victoria from Victure , How is	Inbox	Fwd: Congratulation, You are chosen as a lucky one to get a free floor lamp - support on apeman brand before. Now we have a new product of floor lamp worths \$29.99 start to sell. We want to find ...	3/25/21
Inbox	Fwd: Free Webcam for You - keyword: vitcure webcam (page 1 to 2 to search,	Inbox	Fwd: Free WIFI Dash Cam for You! (Only US) - from the APEMAN Service Team. I hope you are well! Many thanks for your purchasing our product before. Here is a good news to	3/2/21
Inbox	Fwd: (Only US)Testing expensive camera and infrared Thermometer - That is	Inbox	Fwd: Come to be the first to test APEMAN's new item - to test APEMAN's new item To: cnschaal Dear Friend, Good day! This is Linda. Hope this email finds you well. We have launched	1/30/21
Inbox	A Chance to Win Router - Victoria from Victure . How is your day going? I have	Inbox	Fwd: Come to be the fierst to test APEMAN's new item - to test APEMAN's new item To: Dear Friend, Good day! This is Linda. Hope this email finds you well. We have launched a new	1/27/21
Inbox	A Chance to Win Router - Victoria from Victure . How is your day going? I have	Inbox	Come to be the first to test APEMAN's new item - Dear Friend, Good day! This is Linda. Hope this email finds you well. We have launched a	1/16/21
Inbox	Fwd: A Chance to Win Router - Victoria from Victure . Our company launches s	Inbox	Fwd: Come to be the first to test APEMAN's new item - to test APEMAN's new item To: cnschaal Dear Friend, Good day! This is Linda. Hope this email finds you well. We have launched	1/15/21
Inbox	Fwd: A special invitation for you! - From: vitcure Jessica Date: Sat, Jul 25, 2021	Inbox	Come to be the first to test APEMAN's new item - Dear Friend, Good day! This is Linda. Hope this email finds you well. We have launched a	1/15/21
Inbox	Fwd: Free Webcam for You^_ ^ - Lingling from Victure . * So sorry for disturbin	Inbox	Come to be the first to test APEMAN's new item - to test APEMAN's new item To: cnschaal Dear Friend, Good day! This is Nancy. Hope this email finds you well. We have launched	1/14/21
Inbox	Fwd: A special activity for our loyal customer - 26 PM vitcure Jessica > wrote:	Inbox	Fwd: Season's Greetings from APEMAN ! \$0 Camera for You - Greetings from APEMAN ! \$0 Camera for You To: cnschaal Dear Reviewer , This is Susie from APEMAN . So sorry for disturbing you	12/16/20
Inbox	Fwd: Spend 2 minutes to get a Vitcure wifi camera/baby monitor. - PM John V	Inbox	Warm Greetings from APEMAN ! - Susie from APEMAN . Thank you very much for your encouraging our product before. As you are a good reviewer in our recording	12/10/20
		Inbox	Fwd: Could I invite you tp test our dash cam? - Dorsey from Apeman We have recently released a new dual dash cam model and want to invite you to test it out. After you receive	12/9/20
		Inbox	Re: Last Chance before Christmas! Sincere Invitation for Dash Cam Test I - Susan from APEMAN Service Team. Many thanks for > your support our APEMAN product on Amazon. We noticed that you ...	12/3/20
		Inbox	Fwd: Warm Greetings from APEMAN ! (Only US) - Greetings from APEMAN ! (Only US) To: cnschaal - Dear Customer, >>> *This is Susie from APEMAN Service	12/2/20
		Inbox	Fwd: Important Invitation for Touch Screen Front & Rear Dash Cam from APEMAN (US) - Cam from APEMAN (US) To: Hi friend, Hope this email finds you well. This is Helen from APEMAN Dash Cam tea...	11/18/20
		Inbox	Fwd: Come to be the FIRST to test Apeman's NEW Home Cameras! - to test Apeman's NEW Home Cameras! To: Hello friend, This is Jenny from Apeman . Hope this email finds you well. Now i'	11/17/20
		Inbox	Come to be the FIRST to test Apeman's NEW Home Cameras! - Jenny from Apeman . Hope this email finds you well. Now i'm in charge of one of apeman's subbrands--VOGER's	11/17/20
		Inbox	Fwd: Greetings from Alice - Alice from Apeman Service Team. We noticed that you browsed on our product page but didn't place the order. So we would	11/14/20
		Inbox	Fwd: Come to be the FIRST to test Apeman's NEW Home Cameras! - to test Apeman's NEW Home Cameras! To: Hello friend, This is Jenny from Apeman . Hope this email finds you well. Now i'	11/8/20
		Inbox	Fwd: Give us your 2 minutes for a chance to win a cameral - more details :) Sincerely looking forward to hearing from you. Regards, Alice ----- from apeman	10/29/20
		Inbox	FW: Come to be the FIRST to test Apeman's NEW Home Cameras! - to test Apeman's NEW Home Cameras! Hello friend, This is Jenny from Apeman . Hope this email finds you well. Now i'	10/24/20
		Inbox	Remote Control Car , Drones with Camera for Adults-- review free-- company is apeman We recently launched a new listing and would like to invite you to try them for free. We hope that more peo...	10/23/20
		Inbox	Fwd: Give us your 2 minutes for a chance to win a cameral - more details :) Sincerely looking forward to hearing from you. Regards, Alice ----- from apeman	10/17/20
		Inbox	Fwd: LAST 10 QUOTAS to get Apeman binoculars from Amazon US - to get Apeman binoculars from Amazon US To: Dear Customer, This is Zoe from Apeman . To publicize our brand and products, We	9/24/20

Whoa that really escalated

Inbox	Fwd: Free!!!!We invite you test new products-Webcam&Dual Band Wi-Fi Router	Inbox	Fwd: Review - ----- Forwarded from	Inbox	🎉🎉🎉 Register you as our premium member!! PLEASE CHECK!!!! DS02-2P/5.3 - Blake From Treatlife Official ----- Store nbps; Treatlife on Amazon nbps;Facebook Treatlife	5/3/21
Inbox	Fwd: Victure VIP New camera Limited Supply Free Trial - Victure VIP, I'm intere	Inbox	Fwd: Free!!!!We invite you test new prod	Inbox	Re: 🎉🎉🎉 Treatlife Free Smart Color Changing Bulbs and Dimmer Plug to Make Your Home Smarter / SL10-4P 112-6877139-5210602 28.44 DP20-1P 112-6877139-5210602 37.82 pp - nbps; Treatlife ...	4/25/21
Inbox	Fwd: 2.7K VideoCamera Testeinladung Hi	Inbox	Fwd: Citibank has issued a Payout - Pay	Inbox	🎉🎉🎉 Treatlife Free Smart Color Changing Bulbs and Dimmer Plug to Make Your Home Smarter / SL10-4P+DP20-1P / 4.16 - 05 PM Treatlife Support wrote: > Hi > > Have a Nice Day > > Treatlife Free ...	4/24/21
Inbox	Fwd: Hi friends,cover full pp fees , we need US US reviewer, need 5 star review	Inbox	Fwd: Citibank has issued a Payout - Pay	Inbox	🎉🎉🎉 Register you as our premium member!! PLEASE CHECK!!!! DS02-2P/4.14 - Blake From Treatlife Official ----- Store nbps; Treatlife on Amazon nbps;Facebook Treatlife	4/14/21
Inbox	Free WIFI Dash Cam for You! (Only US) - Susie from Victure , So sorry for distur	Inbox	Fwd: Hi friends,cover full pp fees , we ne	Inbox	How's your day with 2 pack 3 way smart dimmer switch? DS02-2P / 3.30th - And all Treatlife members thanks for your great support----- Best	3/30/21
Inbox	Fwd: cnschaal@gmail.com - Lily from Victure Are you interested in reviewing s	Inbox	FW: Sincere Greeting from Susan - us? A	Inbox	Re: Smart Strip Lights/DS02-2/112-1308792-8225005/58/PP - Blake From Treatlife Official nbps; nbps; ----- nbps;Original nbps;-----	3/29/21
Inbox	Fwd: Warm Greetings from Victure !(Only US) - From: Victure Support Date: Tul	Inbox	RE: Sincere Greeting from Susan - Sue fi	Inbox	👋 Welcome to be Our Brand's NEW Product Experience Officer! NL10 0327 ----- Best wishes to you. Monica From Treatlife Official	3/28/21
Inbox	Fwd: Warm Greetings from Victure !(Only US) - From: Victure Support Date: Tul	Inbox	Fwd: P*ree binoculars from the Ape man	Inbox	Re: Smart Strip Lights/DS02-2/112-1308792-8225005/pending - 43 PM Treatlife Support wrote: > Dear buyer, > > Have a good day! > > Thanks for placing the order. Your order	3/26/21
Inbox	Fwd: cnschaal@gmail.com - with our Victure products! 🎉🎉🎉 Are you intere	Inbox	Fwd: Direct Ship FREEBIES!!! - only for A	Inbox	Fwd: Free gift [2 pack 3 way dimmer switch] for you to experience-DS02-2P/3.26th - * Treatlife Support *Date*: March 26, 2021 at 12:00:26 PM EDT *To*: "mark.borowiak2" *Subject*: *Free gift	3/26/21
Inbox	Fwd: \$ 120 Smart Look Test Review Invitation from Victure (USA) - Invitation fir	Inbox	Fwd: RE: Sincere Greeting from Susan -	Inbox	Re:Smart Strip Lights/DS02-2 - 36 AM Treatlife Support wrote: > Dear buyer, > > Good day. > > You can try the keys words "3 way smart dimmer	3/22/21
Inbox	Fwd: RE: Sincere Greeting from Susan - S	Inbox	Fwd: RE: Sincere Greeting from Susan - S	Inbox	👋👋 SL10-2P+SK50-4P/3.2/ 112-2758793-2112212/21.27/PP+112-5951051-6705021/30.09/PP - Michael From Treatlife Official nbps; nbps; ----- nbps;Original nbps;-----	3/20/21
Inbox	Fwd: 4PCS Outdoor WiFi Security Camera System for test! Worth \$190! - ----	Inbox	Fwd: Free Camera for You from APEMAN	Inbox	Re: 🎉🎉🎉 Smart Music Sync Bulbs and Smart Plug Make Your Life More Colorful SL10-2P+SK50-4P/3.2/ 112-2758793-2112212/112-5951051-6705021/pending - 42 AM Treatlife Support wrote: > Dear b...	3/19/21
Inbox	Greetings! Refund from Victure ! - Susie from Victure Support Team. Many thar	Inbox	Congratulation, You are choosen as a lux	Inbox	🎉🎉🎉 Surprise! ! Free gifts for Noble Customer! Smart Bedside Lamp Light up Your Life ! 🎉🎉 NL10 3/14 112-3215116-0572258/PP/ 34.51 - with the Treatlife Smart Product we have given you, coul...	3/19/21
Inbox	Fwd: Kids camera need test - com Victure -Rechargeable-Shockproof-Camo	Inbox	Fwd: Congratulation, You are choosen as	Inbox	🎉🎉🎉 The gift of Treatlife -----Only to our most valued customers! 1 pack dimmer switch &1pack dimmer plug DP20-1/DS01-1 3/2 - :From Treatlife Official nbps; nbps; ----- nbps;O...	3/18/21
Inbox	Fwd: Be the First One to Test Our New Product - Victoria from Victure , How is	Inbox	Fwd: Free WiFi Dash Cam for You! (Only)	Inbox	🎉🎉🎉 Smart Music Sync Bulbs and Smart Plug Make Your Life More Colorful SL10-2P+SK50-4P/3.2 - 15 PM Treatlife Support wrote: > *Hi,* > > *We wish you all the best!!* > > *Now Treatlife is promo...	3/18/21
Inbox	Fwd: (Only US)Testing expensive camera and infrared Thermometer - That is	Inbox	Fwd: Come to be the first to test APEMAN	Inbox	Smart Strip Lights - In one of my recent purchases I had a card telling me to contact support regarding a smart strip	3/17/21
Inbox	A Chance to Win Router - Victoria from Victure , How is your day going? I have	Inbox	Fwd: Come to be the first to test APEMAN	Inbox	Re: 🎉🎉🎉 The gift of Treatlife -----Only to our most valued customers! 4 packs dimmer switch &1pack dimmer plug DP20-1/DS01-4 112-5584274-9609824 65.41 pp - Dear nbps;buyer, Thanks nbps;a...	3/17/21
Inbox	A Chance to Win Router - Victoria from Victure , How is your day going? I have	Inbox	Fwd: Come to be the first to test APEMAN	Inbox	🎉🎉🎉 Surprise! ! Free gifts for Noble Customer! Smart Bedside Lamp Light up Your Life ! 🎉🎉 NL10 3/14 112-3215116-0572258/PP/ 34.51 - with the Treatlife Smart Product we have given you, coul...	3/17/21
Inbox	Fwd: A Chance to Win Router - Victoria from Victure , Our company launches s	Inbox	Come to be the first to test APEMAN 's n	Inbox	🎉🎉🎉 The gift of Treatlife -----Only to our most valued customers! 4 packs dimmer switch &1pack dimmer plug DP20-1/DS01-4 3/11 - 48 AM Treatlife Support wrote: > Dear Customer, > > I am very ha...	3/16/21
Inbox	Fwd: the step to find the product - YES, you can cancel the order, because th	Inbox	Come to be the first to test APEMAN 's n	Inbox	🎉🎉🎉 Surprise! ! Free gifts for Noble Customer! Smart Bedside Lamp Light up Your Life ! 🎉🎉 NL10 3/14 - 22 PM Treatlife Support wrote: > Dear buyer, > > *Congratulations! * > > *Now Treatlife invi...	3/15/21
Inbox	Fwd: A Chance to Win Router - Victoria from Victure , Our company launches s	Inbox	Fwd: Season's Greetings from APEMAN !	Inbox	👋👋 Welcome to be Our Brand's NEW Product Experience Officer! SL20-2P 6th ----- Best wishes to you. Michael From Treatlife Official	3/6/21
Inbox	Refund from Victure - it's just Victure reviews. Adam On Wed, Jul 29, 2020 at t	Inbox	Warm Greetings from APEMAN ! - Susie f	Inbox	🎉🎉🎉 Welcome to our VVIP Club! 🎉🎉🎉---ST30 5th - see the Treatlife TV led backlight on the First nbps;page, Price \$17.99, Please see the attached image. (Note: We only	3/5/21
Inbox	Fwd: A special invitation for you! - From: Victure Jessica Date: Sat, Jul 25, 2020	Inbox	Fwd: Could I invite you tp test our dash c	Inbox	Re: 🎉🎉🎉 Limited Time Offer, First Come First Served 🎉🎉🎉-----SL20-2P 27th/112-61957128-2060207/14.42/pp - Michael From Treatlife Official nbps; nbps; ----- nbps;Original nbps;...	3/1/21
Inbox	Fwd: Free Webcam for You^_ ^ - Lingling from Victure , * So sorry for disturbin	Inbox	Re: Last Chance before Christmas! Sinc	Inbox	🎉🎉🎉 Limited Time Offer, First Come First Served 🎉🎉🎉-----SL20-2P 27th - 30 AM Treatlife Support wrote: > Dear buyer, > > Wish you and your family a great and safe New Year! > > In order	2/28/21
Inbox	Fwd: a special activity for our loyal customer - 26 PM Victure Jessica - > write	Inbox	Fwd: Warm Greetings from APEMAN !	Inbox	🎉🎉🎉 News! Free gift for noble customer! smart fan switch DS02F-IP 2.1 - support, Treatlife would like to invite you to be our VIP customers, and prepare the smart fan switch for you, you are so lu...	2/24/21
Inbox	Fwd: Spend 2 minutes to get a Vitcure wifi camera/baby monitor. - PM Jolin V	Inbox	Fwd: Important Invitation for Touch Scree	Inbox	🎉🎉🎉 News! Free gift for noble customer! smart fan switch DS02F-IP 2.1 - support, Treatlife would like to invite you to be our VIP customers, and prepare the smart fan switch for you, you are so lu...	2/21/21
		Inbox	Fwd: Come to be the FIRST to test Ape man	Inbox	🎉🎉🎉 Treatlife is Promoting! Smart RGB Bulbs Make Your Home Warming SL10-2P/128 - ! Now Treatlife is promoting!! 2 nbps;Pack Smart Bulbs for our VIP members, you are so lucky to have the c...	1/28/21
		Inbox	Fwd: Greetings from Alice - Alice from A	Inbox	🎉🎉🎉 a free gift for lucky customer! Smart LED Strip Lights --ST10 1.12 - use another Amazon account to order. We shall be happy to hear from your letter. Yours faithfully, Bella from Treatlife Official	1/12/21
		Inbox	Fwd: Come to be the FIRST to test Ape man	Inbox	🎉🎉🎉 Christmas Gift is Coming!! ---👋 1 Pack Smart Dimmer Plug 🎉 JUST FOR YOU!!! DPI0-1P 23th - see the Treatlife plug on the first page,Price \$32.99, Please see the attached image. (N...	12/23/20
		Inbox	FW: Come to be the FIRST to test Ape man	Inbox	🎉🎉🎉 Christmas gift is coming!! 4 Packs Smart Color Light Bulbs JUST FOR YOU !! SL11-4P 23th - Hello, Do you want to make your home smarter? Congratulations! We are very happy that you can be...	12/23/20
		Inbox	Remote Control Car, Drones with Camer	Inbox	🎉🎉🎉 Christmas Gift is Coming!! ---👋 2 Packs Smart Tunable White Bulb 🎉 JUST FOR YOU!!! SL20-2P 14th - see the Treatlife bulb on the second or third page,Price \$19.99, Please see the a...	12/14/20
		Inbox	Fwd: Give us your 2 minutes for a chance	Inbox	🎉🎉🎉 Treatlife Newest Christmas Gifts are Coming Now*****SL10-2P 13th - find the Treatlife product on the first page. Price nbps;\$19.99 (We only refund the full amount of designated model	12/12/20
		Inbox	Fwd: LAST 10 QUOTAS to get Ape man bi	Inbox	Welcome to Treatlife VVIP Club-----Experience 4 pack Tunable White Smart Light Bulb for free! SL20-4P 25th - From: Treatlife Support Date: Wed, Nov 25, 2020 at 11:10 AM Subject: Welcome to T...	11/27/20
				Inbox	Re: 🎉🎉🎉 Don't miss the FREE GIFT for you! ---4 pack smart tunable white bulb just for you!!!🎉 SL20-4Pack 17th/113-9283290-5240231/pp/27.92/11.23 - with the Treatlife smart product we have given...	11/23/20
				Inbox	Re: 🎉🎉🎉 Thanksgiving Day Gift is Coming!--- Smart light switch and smart dimmer plug just for you!!!🎉 SSO1S-4/113-8332308-3576247/PP/23TH - with the Treatlife Smart Product, we would really ap...	11/23/20
				Inbox	Re: 🎉🎉🎉 Special Thanksgiving Gift For You!-----DS01-4P-/113-3351789-9079446/pp/23th - with the Treatlife Smart Product, we would really appreciate a product review on Amazon. https://www.a...	11/23/20

But what about the stuff?



Choose your meme adventure, this stuff is suspicious.



03

Cooling & Fermenting

Deep dive in product hardware and software



Adam and Matt's Deep Dive Pub



The
Three T's



Camera
Software



Camera
Hardware



Mesh
Routers



Tekin, Treatlife, Tuya

Treatlife & Tekin products use Tuya IoT Platform → **Evil**

- Plain text, phone #, SSID, device stats, floorplans!
- Device MFG can push silent firmware upgrade at will (of their own compiling, etc)

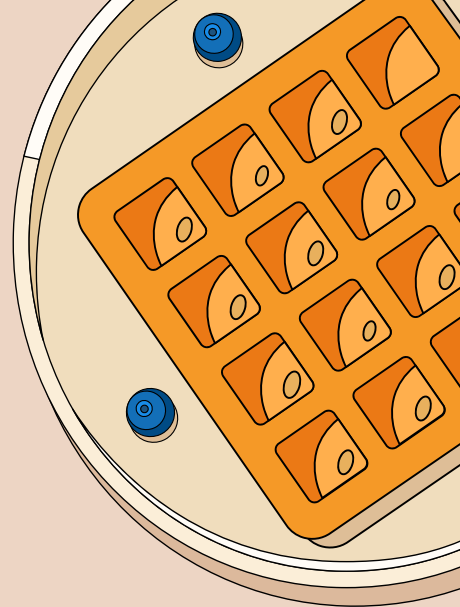
First wave of devices: **ESP8266 processors. Yay!**

- Massive Vulnerability Tuya Convert exploit!

Eventually, this became a patched vulnerability, changed key derivation method.

Michael Steigerwald sources:

- https://media.ccc.de/v/35c3-9723-smart_home_-_smart_hack
- <https://github.com/ct-Open-Source/tuya-convert>



Tekin, Treatlife, Tuya

More devices collected, different processors → **Same FCC Docs?!?**

- Beken-based hardware (WB2S, WP8B, etc)
- Same pinout, but not ESP compatible → **Sad**
- Still using Tuya platform → **Evil**

Pin compatible with ESP32-C3 (and ESP8266-12F)

- Hot air station chip swaps!



Tekin, Treatlife, Tuya

Tuya CloudCutter: Khaled Nassar (et al)

- <https://rb9.nl/posts/2022-03-29-light-jailbreaking-exploiting-tuya-iot-devices/>
- New local keys written – same keys multiple devices
- Device severed from cloud: new keys, no Tuya cloud interaction

New Bekin-compatible firmware!

- <https://github.com/kuba2k2/libretiny>
- https://github.com/openshwprojects/OpenBK7231T_App
- <https://tasmota.github.io/docs/>
- Open-source firmware → **Goodness**

Easily flashed using UART flashing tools!



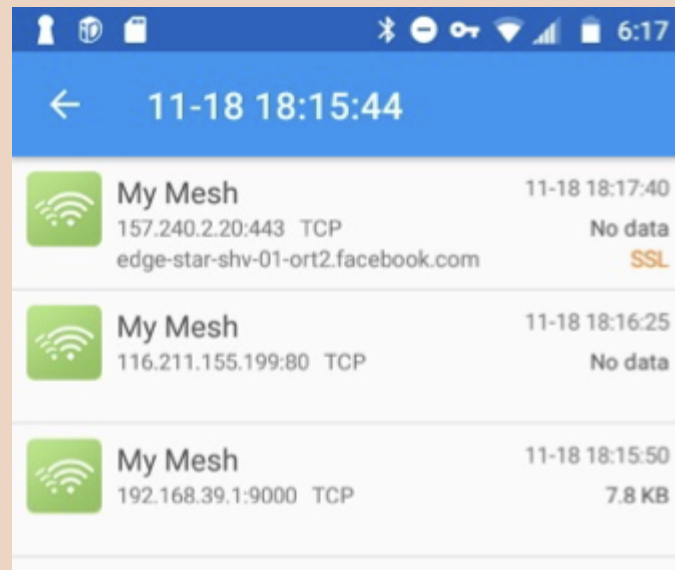
Mesh Routers

- Router configuration requires a phone to set up, they do not have a web interface for the router.
- Nmap shows the following open ports:
 - 5500 (Universal Plug and Play)
 - 9000 (App Interface)
 - 12598 (Used for auto configuring the wifi repeaters)
- The app uses cleartext tcp communication over port 9000 to retrieve serial number and configure the device.
- The serial number is the unchangeable password!



Mesh Routers

- The Android app reaches out to a few places as well... let's investigate.
 - The router, I suppose that makes sense.
 - Also, Facebook!? Why!?
 - And lastly, 116.211.155.199:80...
 - Hmm, I wonder what that is?



The screenshot shows an Android network log with three entries, all from 'My Mesh'. Each entry includes a green Wi-Fi icon, the source IP and port, the protocol, the destination, and the time. The first entry shows a connection to edge-star-shv-01-ort2.facebook.com on port 443 using TCP, with 'No data' and 'SSL' noted. The second entry shows a connection to 116.211.155.199:80 using TCP, with 'No data' noted. The third entry shows a connection to 192.168.39.1:9000 using TCP, with '7.8 KB' noted.

Icon	Source	Protocol	Destination	Time	Details
	My Mesh 157.240.2.20:443	TCP	edge-star-shv-01-ort2.facebook.com	11-18 18:17:40	No data SSL
	My Mesh 116.211.155.199:80	TCP		11-18 18:16:25	No data
	My Mesh 192.168.39.1:9000	TCP		11-18 18:15:50	7.8 KB

Mesh Routers

- The Android app reaches out to a few places as well... let's investigate.
 - The router, I suppose that makes sense.
 - Also, Facebook!? Why!?
 - And lastly, 116.211.155.199:80...
 - Hmm, I wonder what that is?
 - CHINA

An IP WHOIS Lookup determines ownership information of any IP address.

116.211.155.199 **Lookup**

IP WHOIS Lookup Results For 116.211.155.199

% [whois.apnic.net]
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

% Information related to '116.208.0.0 - 116.211.255.255'

% Abuse contact for '116.208.0.0 - 116.211.255.255' is 'anti-spam@chinatelecom.cn'

inetnum:	116.208.0.0 - 116.211.255.255
netname:	CHINANET-HB
descr:	CHINANET Hubei province network
descr:	Data Communication Division
descr:	China Telecom
country:	CN
admin-c:	CH93-AP
tech-c:	CHA1-AP
abuse-c:	AC1573-AP
status:	ALLOCATED PORTABLE
remarks:	
remarks:	To report network abuse, please contact mnt-irt
remarks:	For troubleshooting, please contact tech-c and admin-c
remarks:	Report invalid contact via www.apnic.net/invalidcontact
remarks:	
mnt-by:	APNIC-HM
mnt-lower:	MAINT-CN-CHINANET-HB
mnt-irt:	IRT-CHINANET-CN
last-modified:	2021-06-15T08:05:18Z
source:	APNIC
irt:	IRT-CHINANET-CN
address:	No.31 ,Jingrong street,beijing
address:	100032
e-mail:	anti-spam@chinatelecom.cn
abuse-mailbox:	anti-spam@chinatelecom.cn
admin-c:	CH93-AP



Mesh Routers

- APK investigation
- /cgi-bin/luci/admin/datamanager
- Possible tenda backdoor



Tenda AC15 AC1900 Vulnerabilities Discovered and Exploited

Demonstrating how remote attackers can gain control of the Tenda AC15 AC1900.



Cameras

Several cameras collected (Victure, Voger, Escam, others)

Default/stock software notso good

- Required “interesting” apps to setup
- Long boot time, errors in boot process
- Several on Tuya platform

Moving IP space globally (China -> AWS USA)

Some NOT on Tuya (Escam)

- Interesting P2P connectivity
- Recommended: Paul Marrapese - https://youtu.be/Z_gKEF76oMM
- P2P connections -> huge exposure, unauthenticated access
- P2P connectivity enabled by default when using “PS6 Lite App” setup
- Escam setup app: PS6 Lite App references of “local mode”....gone?
- Camera broadcasts network for “base setup”...
- Connect -> DHCP allocated to client -> examine gateway config.....
- Connect directly to undocumented webif on camera, **no app necessary!**

```
mkdir: can't create directory '/usr/local/pureftpd': File exists
[UDTMediaServer/CUDTMediaServer.cpp]BUILD:Jan  8 2020 16:53:25
[UDTMediaServer/Alexa/CAlexaServer.cpp]BUILD:Jan  8 2020 16:54:02
[UDTMediaServer/MstarAECVerify/CMstarAECVerify.cpp]BUILD:Jan  8 2020 16:53:57
mkdir: can't create directory '/usr/local/pureftpd/etc': File exists
creatSystemUser
Changing password for ftpuser1
New password:
Retype password:
Passwords don't match
passwd: password for ftpuser1 is unchanged
```

P2P	Save
P2P	enabled
UID	Input
status	External network ready



Cameras

Every camera tried to connect out. Some a LOT. Some interesting IP's:

- 119.23.131.xxx (China)
- 120.79.44.0/23 (China)
- 150.136.193.181 Oracle?
- Lots of cloud connections from some cameras

```
LIVE555 Media Server
  version 0.77 (LIVE555 Streaming Media library version 2014.02.10).
Play streams from this server using the URL
  rtsp://0.0.0.0:65534/<filename>
```

Cameras worked with varying success using RTSP/ONVIF

- ESCAM+Foscam best...but still issues

Notable CVE: Live 555 Media Server

- Version .77 running on Foscam camera
- <https://nvd.nist.gov/vuln/detail/CVE-2019-7314>
- <https://github.com/r3dexpl0it/RTSPServer-Code-Execution-Vulnerability>

Live Networks LIVE555 streaming media RTSPServer lookForHeader code execution vulnerability

CVE-2018-4013

Summary

An exploitable code execution vulnerability exists in the HTTP packet-parsing functionality of the LIVE555 RTSP server library. A specially crafted packet can cause a stack-based buffer overflow, resulting in code execution. An attacker can send a packet to trigger this vulnerability.

Work-arounds?

- DHCP reservation without gateway, layer3 ACL, etc.
- UART/JTAG available on most/all cameras (with some digging)
- Open Firmware - <https://github.com/OpenIPC/>, <https://github.com/cjj25/Yi-RTS3903N-RTSPServer>

Cameras

```
showvar - print local hushshell variables
size - determine a file's size
sleep - delay execution for some time
source - run script from memory
sysboot - command to get and boot from syslinux files
test - minimal test like /bin/sh
tftp - boot image via network using TFTP protocol
tftpboot - boot image via network using TFTP protocol
tftpboot - TFTP put command, for uploading files to a server
true - do nothing, successfully
ugzip - Compress gzipfile with hardware IP
unzip - unzip a memory region
version - print monitor, compiler and linker version
OpenIPC # version
```

```
U-Boot 2016.11-g6d2ed0c-dirty (Mar 20 2023 - 13:54:51 +0300)hi3518ev300
arm-himix100-linux-gcc (HC&C V100R002C00B032_20190114) 6.3.0
GNU ld (GNU Binutils) 2.29
OpenIPC #
```

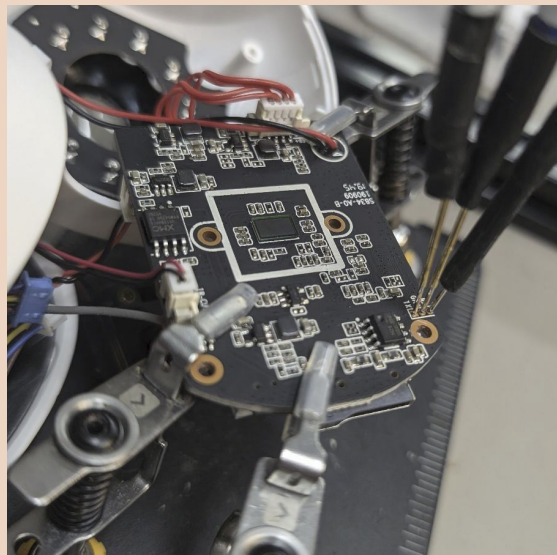
```
openipc-hi3518ev300 login: root
Password:
```

```
.d88888b.      88888888 8888888b. .d8888b.
d88P" "Y88b      888 888  Y88b d88P Y88b
888 888 888      888 888 888 888 888
888 888 888 "88b d8P Y8b 888 "88b 888 8888888P" 888
888 888 888 888 88888888 888 888 888 888      888 888
Y88b. .d88P 888 d88P Y8b. 888 888 888 888      Y88b d88P
"Y88888P" 88888P" "Y8888 888 888 8888888 888      "Y8888P"
888
888
888
888
master+688aaaa, 2024-10-10
```

Please help the OpenIPC Project to cover the cost of development and long-term maintenance of what we believe is going to become a stable, flexible Open IP Network Camera Framework for users worldwide.

Your contributions could help us to advance the development and keep you updated on improvements and new features more regularly.

Please visit <https://openipc.org/sponsor/> to learn more. Thank you.



System startup

Uncompress Ok!

U-Boot 2016.11-svn8496 (Aug 24 2019 - 18:00:33 +0800)hi3518ev300

Relocation Offset is: 03751000

Relocating to 43f51000, new gd at 43f10ef0, sp at 43f10ed0

SPI Nor: NAND: 0 MiB

MMC: Card did not respond to voltage select!

No SD device found !

hisi-sdhci: 0

In: serial

Out: serial

Err: serial

Net: No ethernet found.

*No SD card found!

Hit Ctrl+C key to stop autoboot: 0

hisilicon #

hisilicon #

hisilicon #

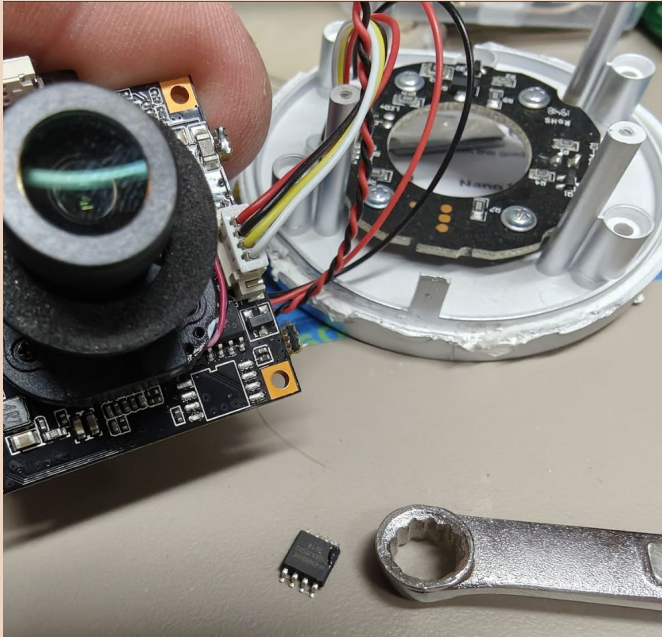


04

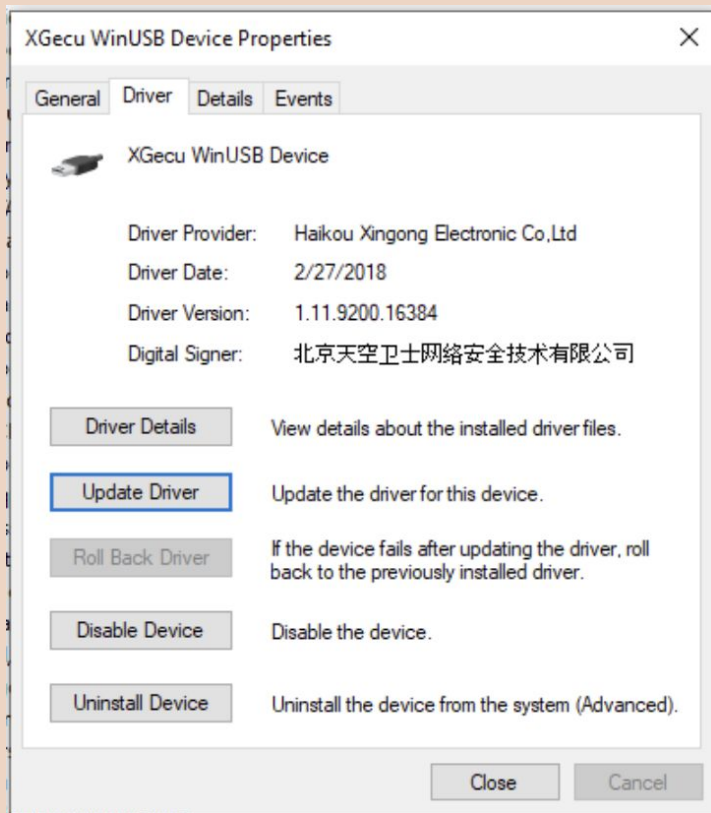
Centrifuge

Scaling our research with GenAI and LLMs

Camera Research



Camera Research



Camera Research



Camera Research

ChatGPT 5 ▾

if i upload a BIN file that consists of firmware from a sur camera, can you extract it with binwalk and tell me about addresses/domains it calls out to or any other interesting filesystem. Also interested in any hard-coded user passwords

Thought for 19s

Absolutely—upload the BIN and I'll statically triage it for you. Here's what I can do right here once the file is attached:

What I'll extract & report

- Any embedded URLs, domains, and IPv4/IPv6 addresses.
- Likely C2 / telemetry endpoints (HTTP(S), MQTT, NTP, DNS-over-HTTPS, etc.).
- Hard-coded usernames/password hints from files like `/etc/passwd`, `/etc/shadow` (has init scripts, and config files).
- Interesting scripts/binaries (startup scripts, update agents, watchdogs), embedded certain suspicious strings.
- Indicators of known filesystems (SquashFS, CramFS, UBIFS, JFFS2) and partition headers

How I'll do it here (no outside tools required)

- Run a deep `strings` pass and regex-scan for:
 - Domains / URLs: `{([a-z0-9-]{1,}\.)*[a-z]{2,}}` and `https?://...`
 - IPv4 / IPv6

What I extracted & analyzed just now

- Top SquashFS candidates (3) + Top JFFS2 candidates (5) were scanned deeply for:
 - `passwd/shadow`-style lines, credential tokens
 - JSON/INI/XML-ish config snippets
 - domains/IPv4/URLs/emails
 - service hints (`onvif/rtsp/p2p/cloud/boa/lighttpd/goahead/etc.`)
 - common file paths (`/etc/passwd`, `/etc/shadow`, `boa.conf`, `wpa_supplicant.conf`, etc.)

Fresh results (over the carved FS blobs)

- Credential artifacts (sample) found in SquashFS blobs:
 - `root:x:0:0:root:/:/bin/sh`
 - `root:$1$6AHjBnTn$LvoexcPTiWwZP5fLFCGdv1:0:0:99999:7:::` ← MD5-crypt hash (salt `6AHjBnTn`)
- Features confirmed from libs/strings inside FS data:
 - ONVIF (`libXSDK_Onvif.so`)
 - RTSP (`libXSDK_Rtsp.so`, `"nRtspPort"`)
 - P2P (`libXSDK_P2P.so`, `"P2P_Server"`, `"stP2PList"`, `"enP2PType"`)
 - Cloud (`libXSDK_Cloud.so`, `"CLOUD_Server"`, `"DevCloudId"`, `"OsscCloudSetting"`, `"bCloudRecord"`, `"bCloudSnapshot"`)
 - Interoperability hooks: `libXSDK_Hik.so`, `"nHikPort"`
 - Boot/Recovery strings: plentiful TFTP strings suggesting loader/recovery behaviors
- Indicators from FS scans: high domain count (likely noisy from data blocks), very few clean URLs. Use the CSV below for triage.

Interesting Findings

- **Credential artifacts (heuristic):**

- Found entries resembling `/etc/passwd` & `/etc/shadow` style lines, including a **root shadow hash**:
 - `root:x:0:0:root:/:/bin/sh`
 - `root:$1$6AHjBnTn$LvoexcPTiWwZP5fLFCGdv1:0:0:99999:7:::` ← **MD5-crypt** (`$1$...`) with salt `6AHjBnTn`
- These may be in a carved filesystem blob; I've included the exact lines in the report so you (or hashcat/john) can attempt offline cracking if desired.

```
## jffs2_candidate_0x000cabd0_7558272.bin (JFFS2)
```

- Size: 7558272 bytes
- SHA256: ``bf3a3193b2cf6a7ee1c971702c9b122db9bdbd33325a079195a39eaa1496b1e0``
- Indicators: 1 IPs, 274 domains, 0 URLs, 0 emails
- Credential-ish lines (sample):
 - ``root:x:0:0:root:/:/bin/sh``
 - ``root:$1$6AHjBnTn$LvoexcPTiWwZP5fLFCGdv1:0:0:99999:7:::``
 - ``"nUserCount":``
 - ``"stUser":``
 - ``"strUserName":``
 - ``"strUserpasswd":``



Introducing the “Kernel”



HARDWARE HACKING VILLAGE

PROJECTS ARE FREE TO DO, SMALL FEE TO TAKE HOME.
(FEE COVERS HARDWARE & SUPPLY COSTS ONLY)

- **BADGE ACTIVITIES (FREE!)**
- **DEEPSEEK DECODER: ON-PREMISE AI (FREE!)**
- **T-MOBILE TEST DRIVE HOTSPOT HACK (\$20)**
- **INDOOR OR OUTDOOR SMART PLUG FIRMWARE FLASH (\$10)**
- **DIY LIGHT STRIP WITH WLED FIRMWARE (\$15)**
- **WIRELESS AP FIRMWARE FLASH: MERAKI --> OPENWRT (\$15)**
- **MESHTASTIC NODE: BUILD+FLASH (\$50)**
- **CRYPTOMINING VILLAGE (FREE!)**

GUIDES AND NOTES AT:
WWW.HACKSPACE.IO/PROJECTS

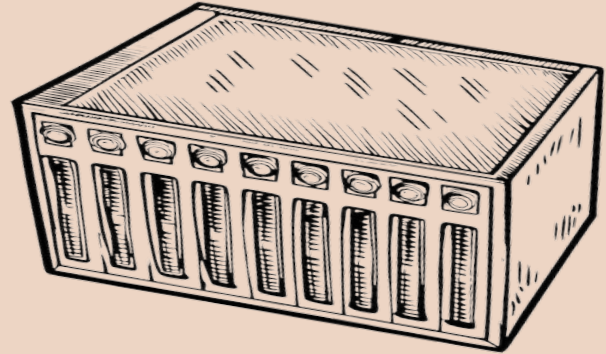
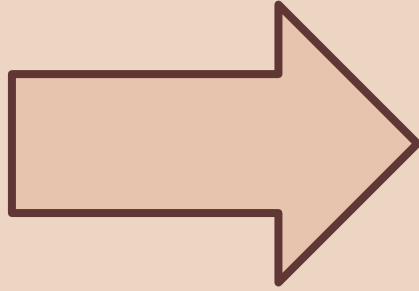


QUESTIONS? PROBLEMS?

YELL FOR A VOLUNTEER FOR ASSISTANCE, WE ARE
HAPPY TO HELP!



Obviously...



We have to throw our \$16 camera firmware at our \$200,000 server.



The “Kernel”

 **Matt Virus** @themattvirus · Mar 28
What's new at the @kernelcon #HHV this year? Introducing: TheKernel.

Specs? @Cisco C245M8 Server..
2x Epyc 9654 Cpus. 192 Cores/384 threads.
24x 64GB DDR5 memory. Total Capacity: 1.5TB.

2x @nvidia A16 gpus, 128GB VRam

We are absolutely running DeepSeek 671B locally.
[Show more](#)



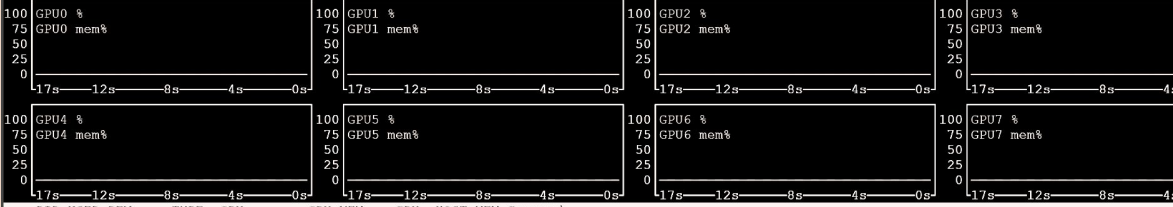
1 1 3 203

```
Device 0 [NVIDIA A16] PCIe GEN 10 4x RX: 450.0 KiB/s TX: 550.0 KiB/s Device 1 [NVIDIA A16] PCIe GEN 10 4x RX: 450.0 KiB/s TX: 550.0 KiB/s
GPU 210MHz MEM 405MHz TEMP 38°C FAN 0% POW 13 / 62 W GPU 210MHz MEM 405MHz TEMP 36°C FAN 0% POW 12 / 62 W
GPU[ 0%] MEM[ 0.374Gi/14.996Gi] GPU[ 0%] MEM[ 0.374Gi/14.996Gi]

Device 2 [NVIDIA A16] PCIe GEN 10 4x RX: 400.0 KiB/s TX: 450.0 KiB/s Device 3 [NVIDIA A16] PCIe GEN 10 4x RX: 450.0 KiB/s TX: 550.0 KiB/s
GPU 210MHz MEM 405MHz TEMP 34°C FAN 0% POW 12 / 62 W GPU 232MHz MEM 405MHz TEMP 32°C FAN 0% POW 11 / 62 W
GPU[ 0%] MEM[ 0.374Gi/14.996Gi] GPU[ 0%] MEM[ 0.374Gi/14.996Gi]

Device 4 [NVIDIA A16] PCIe GEN 10 4x RX: 400.0 KiB/s TX: 500.0 KiB/s Device 5 [NVIDIA A16] PCIe GEN 10 4x RX: 450.0 KiB/s TX: 500.0 KiB/s
GPU 210MHz MEM 405MHz TEMP 34°C FAN 0% POW 11 / 62 W GPU 232MHz MEM 405MHz TEMP 35°C FAN 0% POW 11 / 62 W
GPU[ 0%] MEM[ 0.374Gi/14.996Gi] GPU[ 0%] MEM[ 0.374Gi/14.996Gi]

Device 6 [NVIDIA A16] PCIe GEN 10 4x RX: 450.0 KiB/s TX: 450.0 KiB/s Device 7 [NVIDIA A16] PCIe GEN 10 4x RX: 350.0 KiB/s TX: 500.0 KiB/s
GPU 232MHz MEM 405MHz TEMP 32°C FAN 0% POW 11 / 62 W GPU 232MHz MEM 405MHz TEMP 30°C FAN 0% POW 11 / 62 W
GPU[ 0%] MEM[ 0.374Gi/14.996Gi] GPU[ 0%] MEM[ 0.374Gi/14.996Gi]
```



PID	USER	DEV	TYPE	GPU	GPU MEM	CPU	HOST MEM	Command
-----	------	-----	------	-----	---------	-----	----------	---------

“A high-end, powerful machine, purpose built for AI analysis”

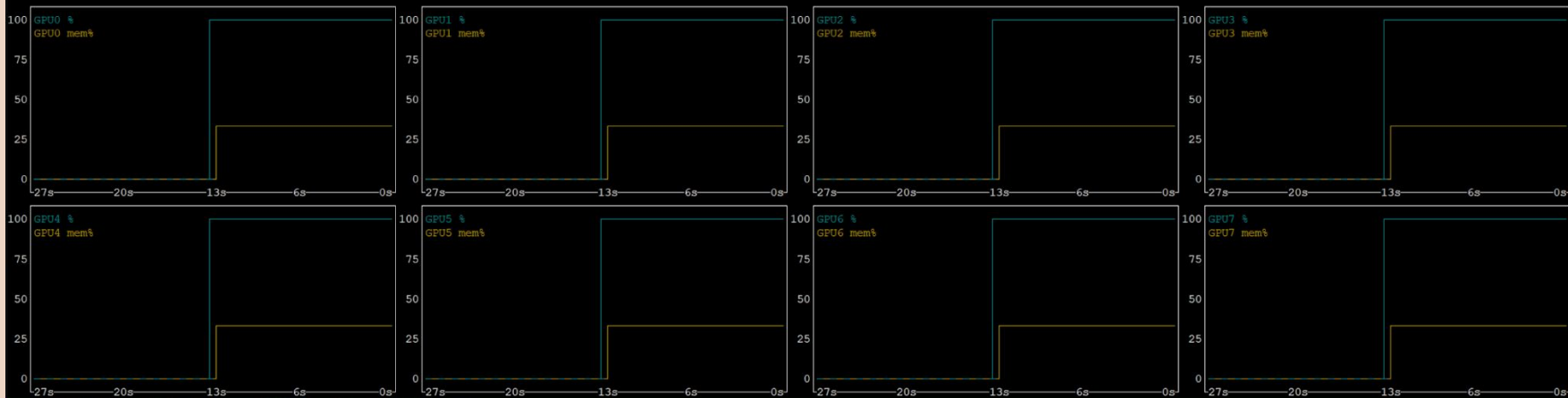


Hashcat running on The Kernel

```
Device 0 [NVIDIA A16] PCIe GEN 4@ 4x RX: 600.0 KIB/s TX: 750.0 KIB/s Device 1 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.416 MIB/s TX: 550.0 KIB/s Device 2 [NVIDIA A16] PCIe GEN 4@ 4x RX: 650.0 KIB/s TX: 750.0 KIB/s
GPU 1755MHz MEM 6251MHz TEMP 68°C FAN 0% POW 48 / 62 W GPU 1755MHz MEM 6251MHz TEMP 68°C FAN 0% POW 47 / 62 W GPU 1755MHz MEM 6251MHz TEMP 68°C FAN 0% POW 43 / 62 W
GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi] GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi] GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi]

Device 3 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.221 MIB/s TX: 500.0 KIB/s Device 4 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.221 MIB/s TX: 750.0 KIB/s Device 5 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.221 MIB/s TX: 750.0 KIB/s
GPU 1755MHz MEM 6251MHz TEMP 56°C FAN 0% POW 43 / 62 W GPU 1755MHz MEM 6251MHz TEMP 62°C FAN 0% POW 44 / 62 W GPU 1755MHz MEM 6251MHz TEMP 65°C FAN 0% POW 44 / 62 W
GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi] GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi] GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi]

Device 6 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.172 MIB/s TX: 700.0 KIB/s Device 7 [NVIDIA A16] PCIe GEN 4@ 4x RX: 1.270 MIB/s TX: 500.0 KIB/s
GPU 1755MHz MEM 6251MHz TEMP 57°C FAN 0% POW 42 / 62 W GPU 1755MHz MEM 6251MHz TEMP 52°C FAN 0% POW 42 / 62 W
GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi] GPU[|||||||||||||||||99%] MEM[||||| 4.643Gi/14.996Gi]
```



PID	USER	DEV	TYPE	GPU	GPU MEM	CPU	HOST MEM	Command
1546951	N/A	0	Compute	99%	4364MiB	28%	801%	12742MiB hashcat hashfile -a 3
1546951	N/A	1	Compute	99%	4364MiB	28%	1035%	12742MiB hashcat hashfile -a 3
1546951	N/A	2	Compute	99%	4364MiB	28%	1147%	12742MiB hashcat hashfile -a 3
1546951	N/A	3	Compute	99%	4364MiB	28%	0%	12742MiB hashcat hashfile -a 3
1546951	N/A	4	Compute	99%	4364MiB	28%	1156%	12742MiB hashcat hashfile -a 3
1546951	N/A	5	Compute	99%	4364MiB	28%	1004%	12742MiB hashcat hashfile -a 3
1546951	N/A	6	Compute	99%	4364MiB	28%	510%	12742MiB hashcat hashfile -a 3
1546951	N/A	7	Compute	99%	4364MiB	28%	1155%	12742MiB hashcat hashfile -a 3

Success

password is yunyi666



yunyi: Mandarin

- *cloud*
- *free as a cloud*
- *elegant [brand]*



Victure NX200-TX

Other DeepSeek Interesting Findings

squashfs_squashfs	b1380d8a795d739a63fe8a13efdbc840b0e2c1c78d0c8c22da086ace94d01c72	domain	s.su	
squashfs_squashfs	b1380d8a795d739a63fe8a13efdbc840b0e2c1c78d0c8c22da086ace94d01c72	domain	sn.bin	
squashfs_squashfs	b1380d8a795d739a63fe8a13efdbc840b0e2c1c78d0c8c22da086ace94d01c72	domain	sts.dvr163.com	
squashfs_squashfs	b1380d8a795d739a63fe8a13efdbc840b0e2c1c78d0c8c22da086ace94d01c72	domain	syscaps.json	

domain	carved_xz_00_decompressed	your.3322.org
domain	carved_xz_00_decompressed	members.3322.org
email	carved_xz_00_decompressed	ctnet@mycdma.cn



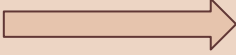
05

Carbonation

Cautionary Tales from our experiences

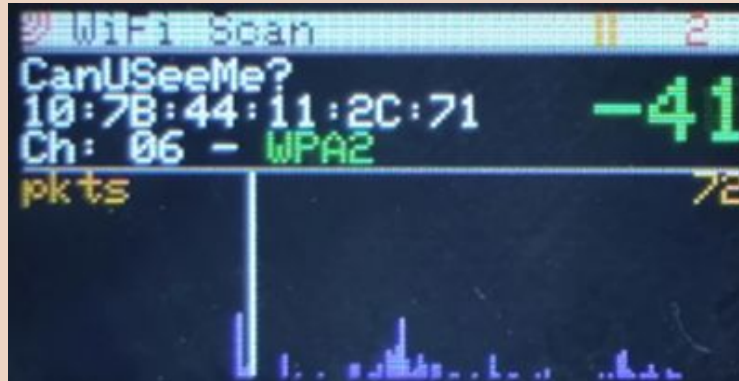


Cautionary Tale: Bed Bug

- 2x strange SSID showed up seemingly randomly. 
- Investigated (*lightly*) over ~1.5 years, with no results.
- Connecting yielded no details, port 80 open.
- DHCP running, address handed out.
- Enter **DOPESCOPE!**



WMB07FAC
WMB07E58



Cautionary Tale: Bed Bug

Offending Hardware

- Adjustable bed base unit.

Interesting Detail

- Previously investigated, identified hardware on bed base did not align with wifi hardware in manual. Also, did not order wifi adjustable base, verified through purchase order.
- **But...** the bed is indeed adjustable via wifi!



LESSON LEARNED

Even valid/trusted/clandestine hardware can be odd and behave in unexpected ways.

Cautionary Tale: Oh Baby

- Rogue SSID on network as a random string of characters and numbers.
- Unauthenticated access, didn't appear to do anything, nor did it have standard ports.
- I had only plugged in so many things, so I was able to figure it out.
- Solution: return all, buy a model that specifically said it didn't use wifi and verify the products claims.



[Order details](#)
Voguer Baby Monitor
Night Vision, Co
Voguer



[Order details](#)
Victure Dual
Audio, Motion
Victure



[Order details](#)
Victure 1080P B
Victure

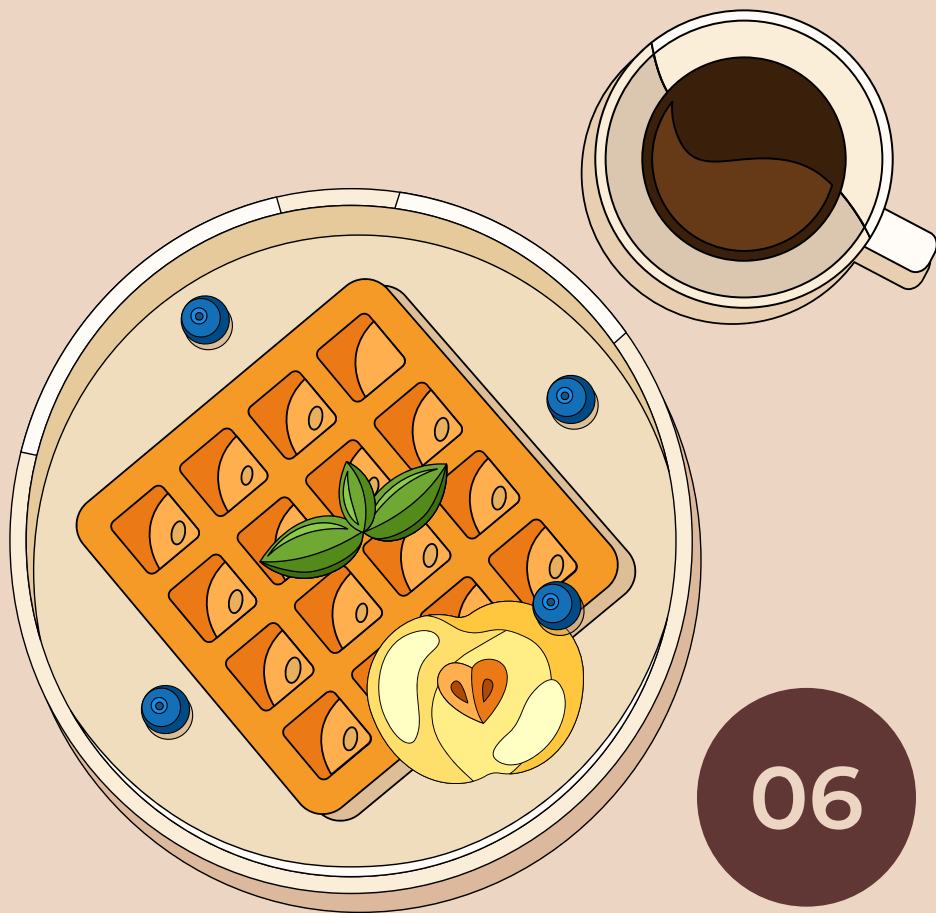


[Order details](#)
[New Version]
Detection/2-
APEMAN



LESSON LEARNED

Do not add hardware to your setup, without vetting it and ensuring it performs correctly.



06

Bright Tank

Now, how do you purchase online safely?

White Labels

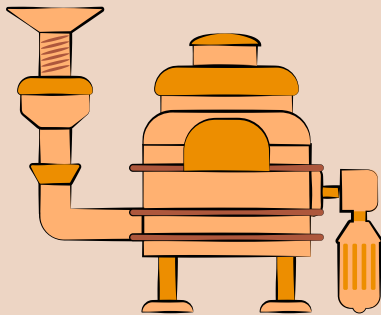


Most of these brands are **white labels**, which means they relabel their product when their storefront gets shutdown or they need a brand refresh.

- Oftentimes the firmware may differ slightly, but the hardware is exactly the same and has the same flaws and vulnerabilities.
- ***NOTE - White label hardware is typically supplied by Tuya.***



Lessons Learned



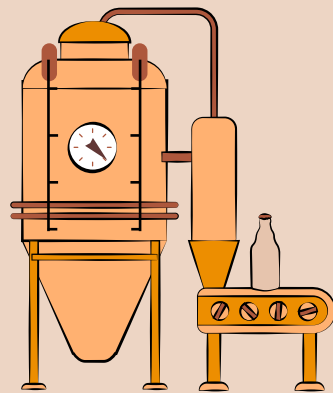
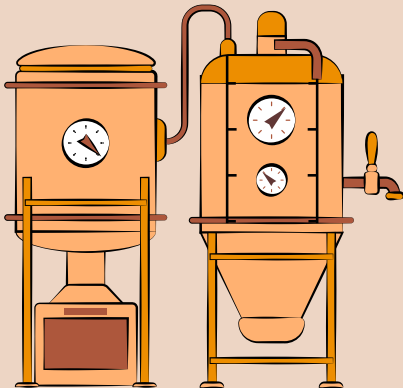
Pay Attention

If something is too good to be true, it probably is.



Exercise Caution

Always test untrusted hardware in a safe environment, before putting in home ops.



Be Skeptical

Be wary of online reviews. Approach with skepticism, not all of them are legitimate.

How to spot Fake Reviews

5 stars, every time, no exceptions

No negative comments

ALWAYS has picture

★★★★★ Excellent dimmer -highly functional

December 7, 2019

Verified Purchase

The TM Innovation digital Bluetooth thermometer is dependable it is a great value. Excellent value for daily use. It delivers reliable temperature measurements with ease. This is the best thermometer I have ever used, i really like it a lot! It is a great addition to any healthcare kit.



Generic: "very good" but no detail

Overly enthusiastic!

Sometimes not related to product at all!

07

Bottling

What's next, wrap up, Santé!



Moving to Facebook Groups

 **Kaivy** <154291309@qq.com>
to me ▾

Hi

Thanks for your quick reply.

Sorry, due to the upcoming promotional festival, we are currently in short supply, so the **test** quota has been reduced.

If you have Facebook, please join our **test** group, we will post more free quality products in it later.

Facebook group:
<https://www.facebook.com/groups/kaivyfriend/>

Thanks again, and look forward to cooperating with you in the future.

Have a nice day!

Best regards,
Kaivy

----- 原始邮件 -----

发件人: "Adam Schaal" <aschaal1263@gmail.com>;
发送时间: 2021年4月29日(星期四) 上午6:52
收件人: "Kaivy" <154291309@qq.com>;
主题: Re: Computer Tablet **Test** Invitation

 **xin liang** [redacted]
to me ▾ Thu, Jul 15, 2021, 8:43 PM ☆ ↶ ⋮

Hello, friend

Thank you for your reply. I am to be happy

The steps to test this product are:

1. Search keyword: Robot Vacuum and find our product. It's on page 4-5, thank you for your patience, it will take you a little time.
This picture is the main picture of our product, priced at \$212.49 with \$30 coupon. (please use the coupon)



2. After you find the product, please check the detail page and add it to your shopping cart, and help me ask 5 questions about my product on Amazon, all these actions are for your account security.
3. Please place the order directly, after you finish the order, please send me your order screenshot + order number, and also send your PayPal email.
4. After you receive the **goods**, and please review with some pictures or video on Amazon please contact me and I will return the full amount for you (include 100% pp fee no tax)

Are you willing to accept such a step?

Meanwhile, I very sincerely invite you to join our official **FB group**.
[https://www.facebook.com/groups/\[redacted\]](https://www.facebook.com/groups/[redacted])

Any questions, we're all in!



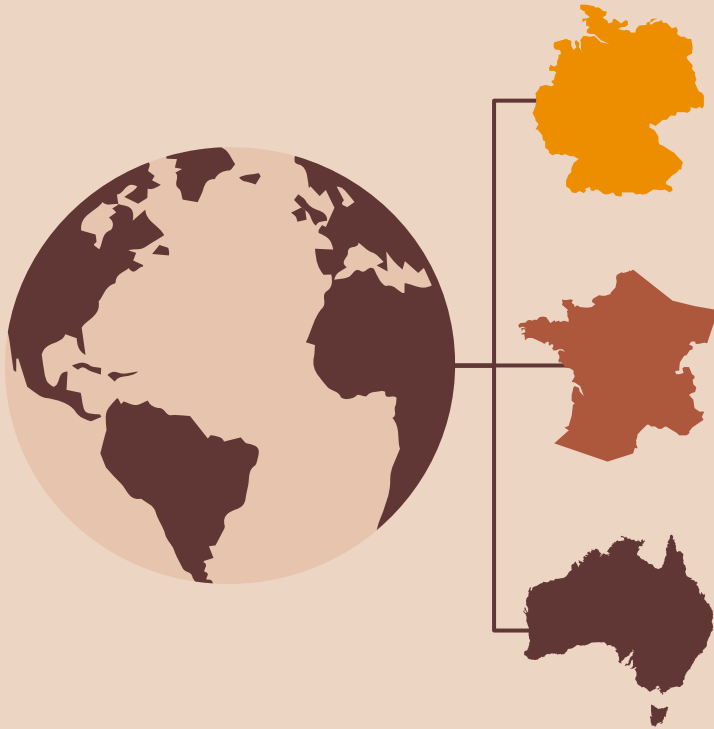
Some Vendors Are Doing It Right



- Offers a “research fee” for purchasing their camera and reviewing.
- Never asked for an online review, just asked for replies to a product research email.
- Product cost \$80, research fee was \$140.
- Still able to pass this around to the cabal.



Global Problem



These products have become common; they're cheap and highly ranked on marketplaces.

The people who suffer the most are local shop owners or public services.

In fact, we've been to a few of those types of places on this trip.



Example: Tapo in Coffee Shop in Paris



Example: TP-Link Plug in MOCA (Paris)



Example: NK Bodega in Paris.



Example: Hikvision in Ghent.



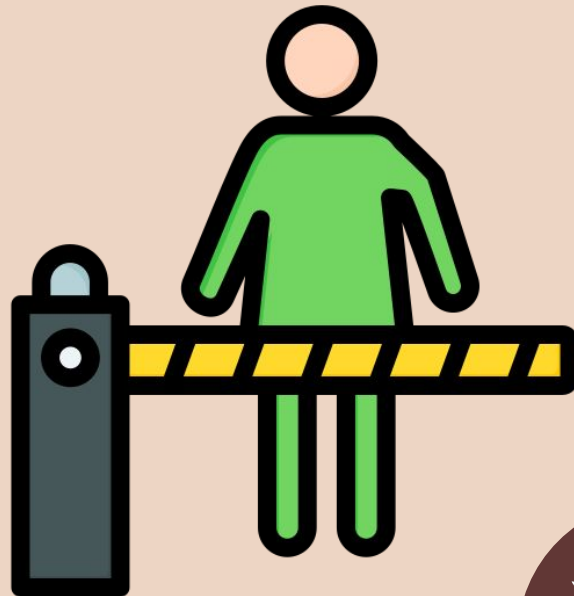
This is how you end up on Shodan



Our Long-Term Goal - Accessibility

This project will culminate with our long-term goal of **making firmware analysis more accessible.**

The barrier-of-entry for analyzing firmware for bugs, vulnerabilities, and general shittiness is **too high.**



Step 1: Making this Reusable (locally)

```
fw_analysis.py
1  #!/usr/bin/env python3
2  """
3  fw_analysis.py
4
5  Expanded firmware analysis helper:
6  - Carves candidate blobs from BIN images (SquashFS, XZ, LZMA, gzip, JFFS2 markers)
7  - Attempts nested decompression (gzip, xz, lzma) in-Python (safe caps)
8  - If `unsquashfs` is available, unsquashes SquashFS blobs into `unsquashed/`
9  - Recursively scans carved blobs and extracted filesystem trees for IOCs and suspicious artifacts:
10     * domains, IPv4s, URLs, emails
11     * /etc/passwd, /etc/shadow-like lines
12     * init.d references, service config paths
13     * PEM/private key beginnings
14     * telnet/ssh/dropbear mentions and updater/p2p/cloud keywords
15  - Writes outputs:
16     OUT_DIR/
17     | carved/
18     |   extracted/      (nested decompressed artifacts)
19     |   unsquashed/     (if unsquashfs succeeds)
20     |   iocs/           (CSV lists)
21     |   REPORT.md
22
23  Usage:
24  python3 firmware_finder_extended.py -i firmware.bin -o analysis_out
25
26  Requirements:
27  - Python 3.8+ (3.10 recommended)
28  - Optional: unsquashfs (squashfs-tools) on PATH to expand SquashFS blobs
29  """
```

We don't want this to be a one-time scan that we created.

So, it's been moved to GitHub. This is a scrappy version made by DeepSeek and us with love.

 https://github.com/mattvirus/fw_analysis



Step 2: Expanding our Coverage

Keep your eyes on our GitHub and social media profiles as we work on what's next.

A little preview...

- Firmware Analysis and Inspection
MCP Server
- Potentially opening sovereign
DeepSeek scanning to our
community.

A terminal window showing the FastMCP 2.0 startup information. At the top, the text 'FastMCP 2.0 (*)' is displayed in a green, stylized, outlined font. Below this, the text 'FastMCP 2.0' appears in a standard white font. The terminal then lists several configuration details: 'Server name: binwalk-mcp' with a computer icon, 'Transport: STDIO' with a hexagon icon, 'FastMCP version: 2.12.2' with a version icon, and 'MCP SDK version: 1.13.1' with a heart icon. At the bottom, it provides links for 'Docs: https://gofastmcp.com' and 'Deploy: https://fastmcp.cloud', each accompanied by a small icon.

```
FastMCP 2.0 (*)  
  
FastMCP 2.0  
  
Server name: binwalk-mcp  
Transport: STDIO  
  
FastMCP version: 2.12.2  
MCP SDK version: 1.13.1  
  
Docs: https://gofastmcp.com  
Deploy: https://fastmcp.cloud
```



Thank You

Any Questions?

Adam Schaal
@clevernyyyy

Matt Virus
@themattvirus
@hackspaceio



Credits: This presentation template was created by Slidesgo, and includes icons by Flaticon, and infographics & images by Freepik