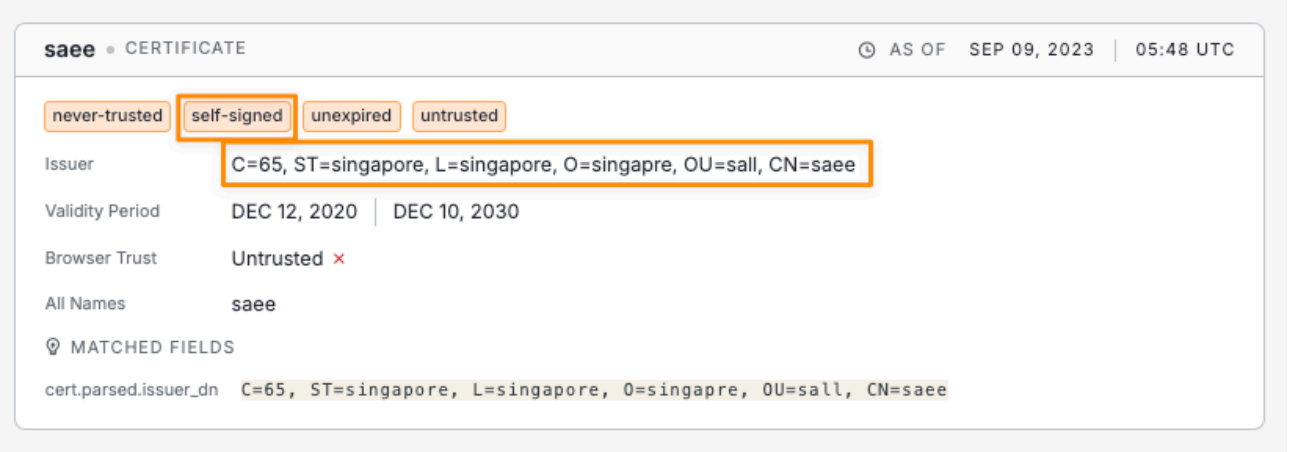
Unpacking the BADBOX Botnet with Censys

By Jean Pierre Ruiz Ocampo

Published: 2025-02-04 · Archived: 2026-04-05 22:47:29 UTC

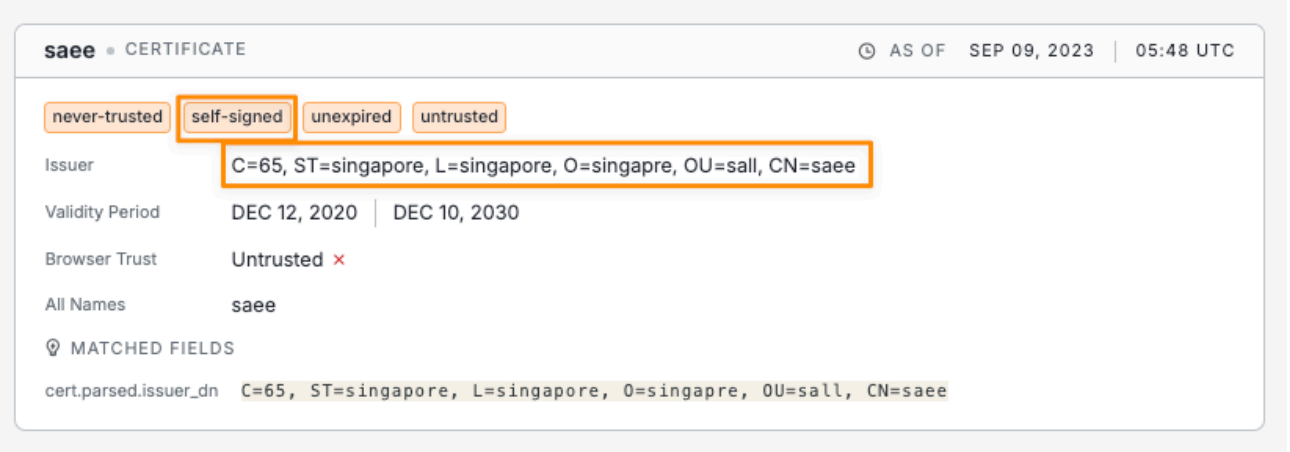


Executive Summary: BADBOX is a newly discovered botnet targeting both off-brand and well-known Android devices—often with malware that potentially came pre-installed from the factory or further down in the supply chain. Over 190,000 infected devices have been observed so far, including higher-end models like Yandex 4K QLED TVs. Using Censys, I identified a suspicious SSL/TLS certificate common to BADBOX infrastructure, revealing five IPs and numerous domains, all using the same certificate and SSH host key. This strongly indicates a single actor controlling a templated environment. The sheer scale and stealthy nature of BADBOX underscore the critical need to monitor supply chain integrity and network traffic.

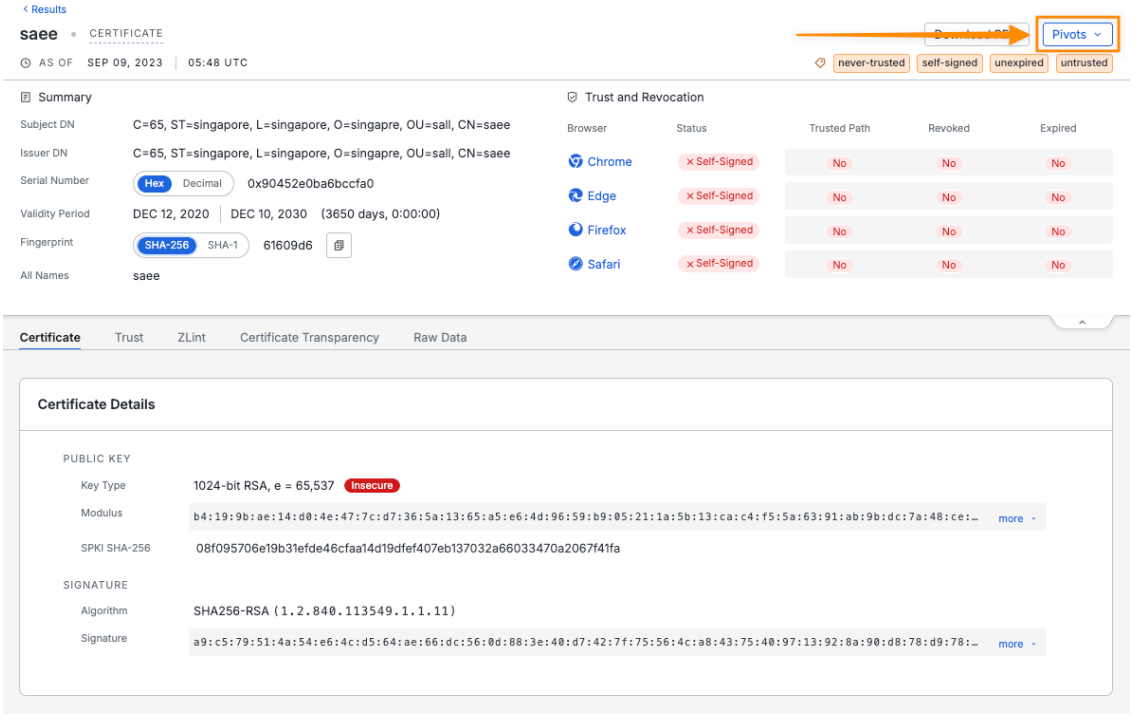
I've been watching this emerging threat for a while, and on the surface, it sounds like just another Android malware campaign. The twist? BADBOX often comes baked into the firmware, so people are unboxing new devices that are already compromised before they even join a network. Researchers from BitSight recently highlighted the huge number of devices communicating with BADBOX servers, suggesting a full-blown supply chain compromise that goes well beyond a typical sideloaded malware incident. Below, I'll walk you through how I used Censys to track the certificate in question and map out the associated IPs and domains.

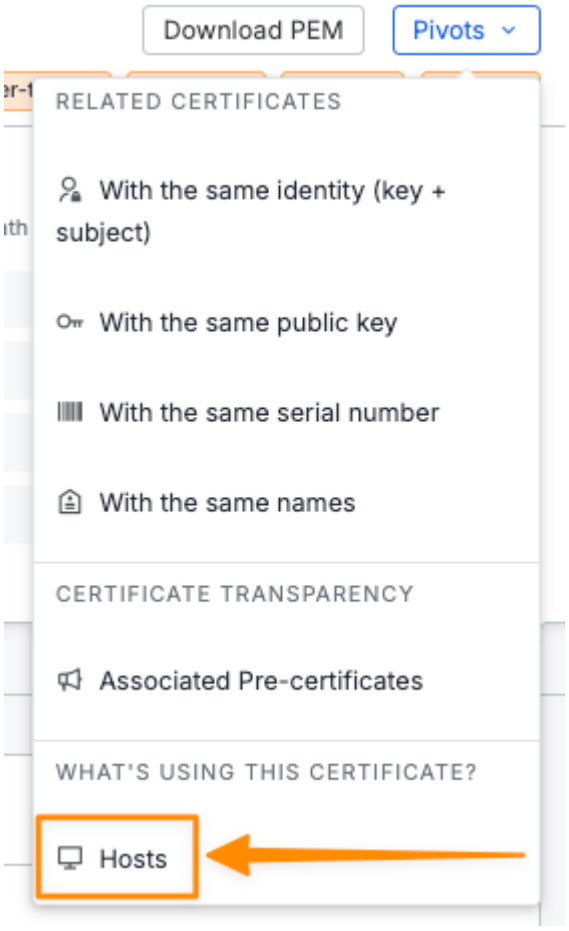
This scale piqued my curiosity—particularly the part about a common certificate that's been spotted in the wild. Armed with this bit of intel on the certificate's issuer DN, I turned to the Censys Internet Intelligence Platform to see if I could track down any additional evidence. The issuer DN in question is: "C=65, ST=singapore, L=singapore, O=singapre, OU=sall, CN=saee" which I converted into the following Certificate query to find the exact certificate used by BADBOX operators.

There was a single result that matched that criteria, which is a strong indicator of a single entity (or a small group) behind the widespread malware injection.

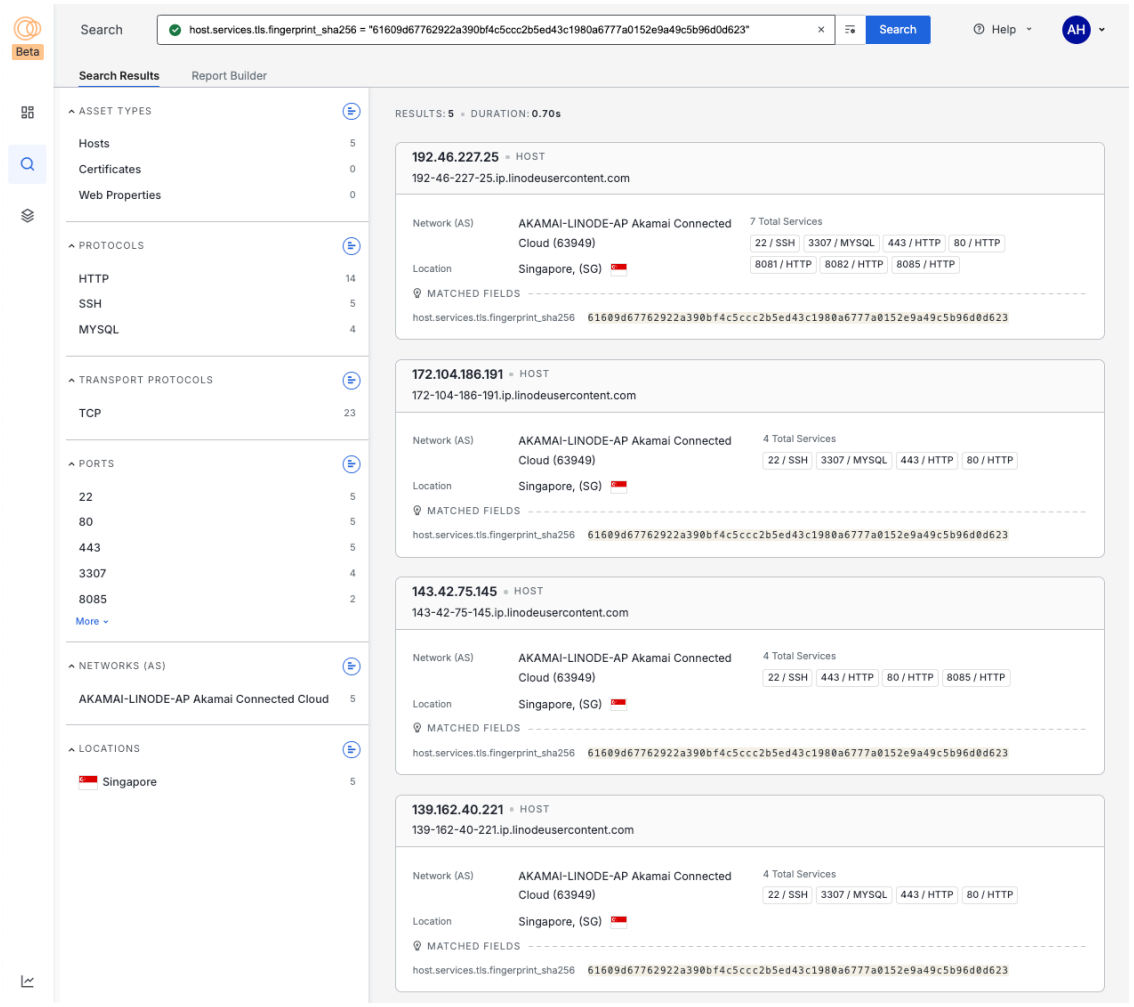


This made me curious about what hosts this certificate is presented on so I entered the pivot menu.

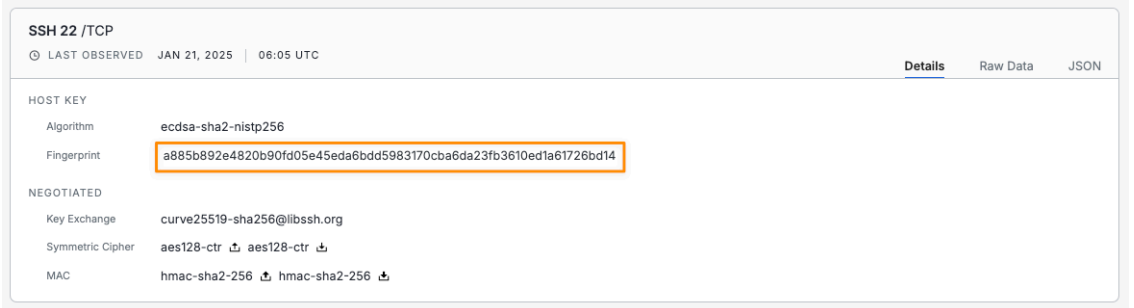




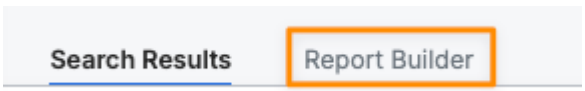
This pivot produced the following query, which searches for the certificate's SHA-256 fingerprint.

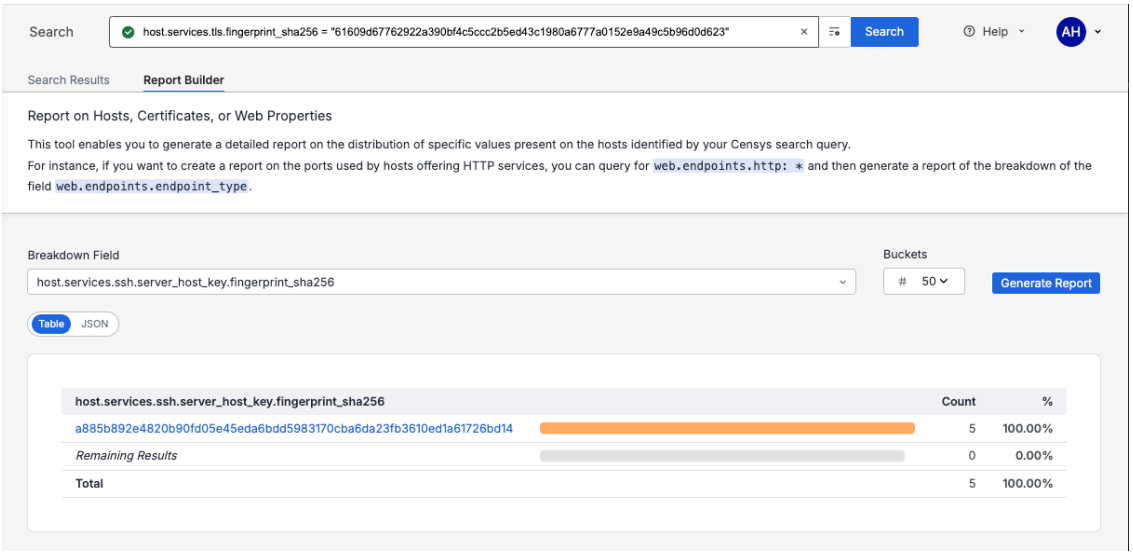


This returned five IP addresses that are presenting that certificate, all from Singapore and all from the Akamai ASN. I was curious what other attributes they share and I noticed that they all have port 22 SSH open. Here is one of those services.



To track if the same SSH Host Keys are used, we can do a report on the Host Key Fingerprint field “host.services.ssh.server_host_key.fingerprint_sha256”. To do a report, click the “Report Builder” tab.

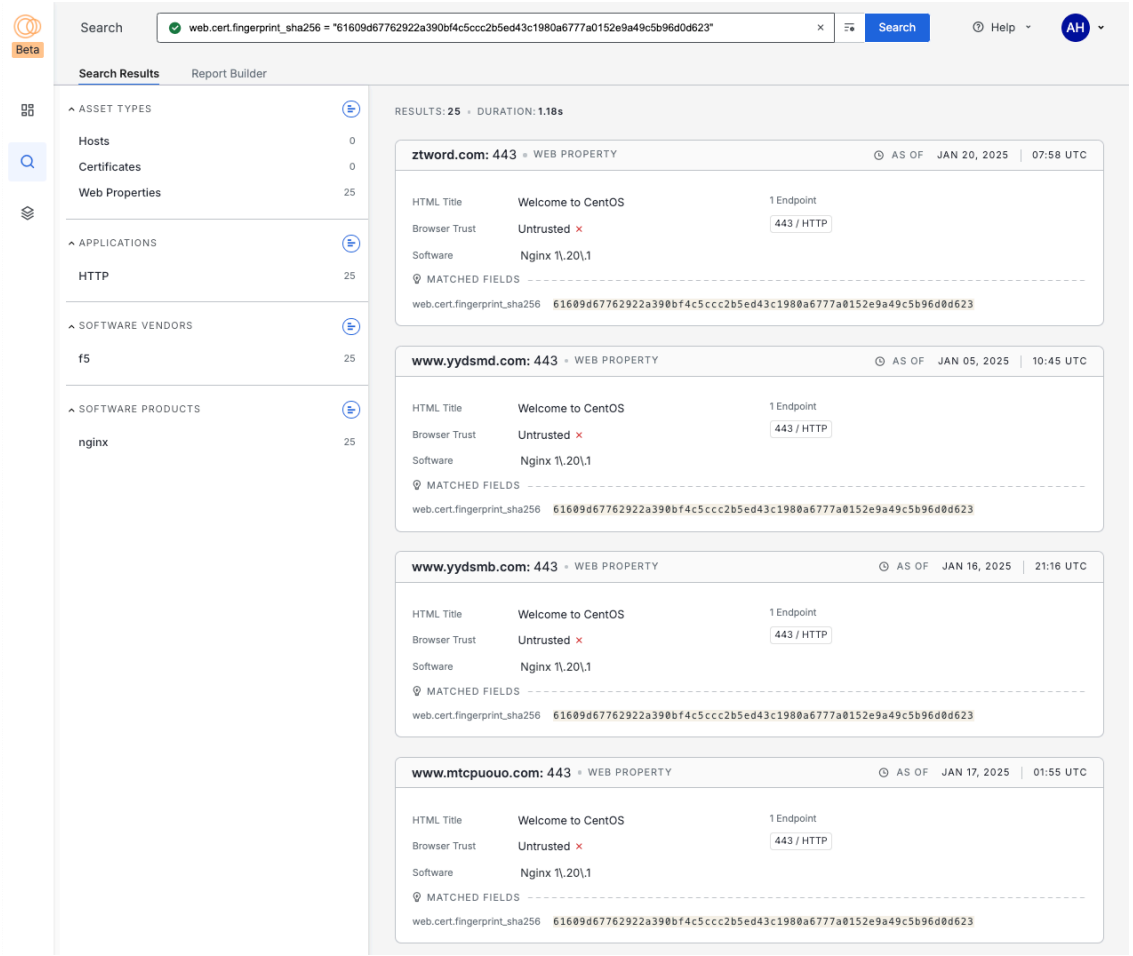




As you can see, all five IPs share the same SSH Host Key suggesting that these instances were templated. By clicking on the report's table I can pivot into that query.

Which I would clean up to be the following query:

However, I was also interested in the number of domains that also present this certificate.



Interestingly enough, all 25 appear to be running nginx 1.20.1 on CentOS. From here I could either make a collection to track all of these indicators or simply extract the current instances. Below is the final query with all the above indicators

host.services.tls.fingerprint_sha256 = “61609d67762922a390bf4c5ccc2b5ed43c1980a6777a0152e9a49c5b96d0d623”

or host.services.ssh.server_host_key.fingerprint_sha256 = “a885b892e4820b90fd05e45eda6bdd5983170cba6da23fb3610ed1a61726bd14”

or web.cert.fingerprint_sha256 = “61609d67762922a390bf4c5ccc2b5ed43c1980a6777a0152e9a49c5b96d0d623”

Indicators

IPs

139.162.36[.]224

139.162.40[.]221

143.42.75[.]145

172.104.186[.]191

192.46.227[.]25

172.104.178[.]158

Domains

bluefish[.]work

www.bluefish[.]work

cool.hbmc[.]net

giddy[.]cc

www.giddy[.]cc

jolted[.]vip

joyfulxx[.]com

msohu[.]shop

www.msohu[.]shop

mtcpuouo[.]com

www.mtcpuouo[.]com

pasiont[.]com

sg100.idcloudhost[.]com

www.yydsmb[.]com

www.yydsmd[.]com

ztword[.]com
tvsnapp[.]com

pixelscast[.]com

swiftcode[.]work

old.1ztop[.]work

cast.jutux[.]work

home.1ztop[.]work

www.jolted[.]vip

AUTHOR

Aidan Holland

Senior Security Researcher

Aidan Holland is a Senior Security Researcher with Censys ARC, where he specializes in threat intelligence and internet-wide security research. His work focuses on identifying and analyzing malicious infrastructure, tracking threat actors, and developing tools for security analysis at scale. Aidan is an active contributor to the open source security community, building and maintaining tools for threat hunting, data analysis, and security automation.
