DeepSec 2017 Talk: Next-Gen Mirai Botnet – Balthasar Martin & Fabian Bräunlein

Posted on **September 27,2017** by **sanna**

While you were living in a cave, devices took over the world and got connected to the network. This is the state of affairs we live in right now. As long as nothing happens we don't notice anything about it. The Mirai (??) botnet changed this all of a sudden. Consumer devices were drafted into an army of bots. Thanks to the proliferation of networked devices such as cameras, home routers, and others the botnet was very successful. The code was designed to run on embedded devices and is even online for inspection. Let's take a look at how to improve Mirai.

Badly secured embedded devices enabled the largest DDoS attack on critical networks seen to date: The Mirai attacks in 2016 were largely pegged on Internet-exposed telnet with default credentials. While such telnet accounts are hopefully on their way out, Balthasar and Fabian had a look at the next available hacking options to compromise masses of IoT devices. It turns out that IP cameras can still be compromised remotely in many other ways – even if they are not exposed directly to the internet. In particular, they found issues in communication protocols, control servers and infrastructure design. Balthasar Martin and Fabian Bräunlein found such next-gen Mirai vulnerabilities, and they will demonstrate a number of them. After seeing what we saw, they say, you will have little doubt that there will always be a bot army of compromised embedded devices.

We asked Balthasar and Fabian a few questions about their topic of interest.
Please tell us the top 5 facts about your talk.

Without disclosing all interesting discoveries, here are four that we are really proud of:

1. *Cloud services expose our devices to the Internet, even if we put them behind a firewall.*
2. *Cameras come in many shapes and brands, but most of them use one of few cloud services.*
3. *It's 2017 and people still invent proprietary protocols with big security holes.*
4. *We learned two things from Mirai that turn out to be insufficient: "do not expose your device directly to the Internet" and "change any default credentials".*

How did you come up with it? was there something like an initial spark that set your mind on creating this talk?

The Mirai attacks last year caught our attention. Given that they were based on open telnet with default passwords, we were curious to know what else was hidden behind the complexity of those devices.

Why do you think this is an important topic?

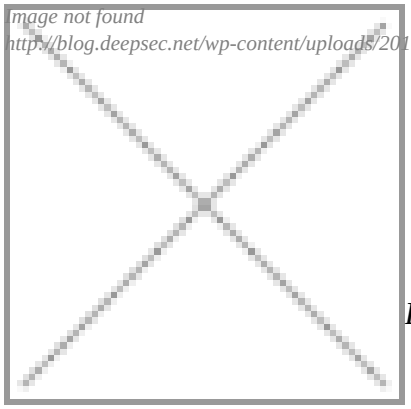
The discrepancy between what is exploited (consumer devices) and who suffers from attacks (big companies, targeted individuals) is interesting to think about. Device owners usually don't notice that they are being hacked. On the other end, the victims of DDoS attacks don't control the device's security. We think public awareness is especially important here.

Is there something you want everybody to know - some good advice for our readers maybe?

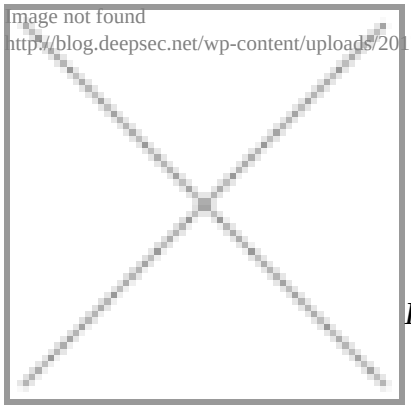
You may want to stay away from cloud-connected devices. In the case of cloud IP cameras, even when everything is properly secured, the vendors can still access your camera feeds, as all information is transmitted via their servers without end-to-end encryption.

A prediction for the future - what do you think will be the next innovations or future downfalls when it comes to particularly your field of expertise / the topic of your talk?

Following the current trend, we think there will be device choices with solid security. Hopefully consumers start considering security more and if so, are able to recognize secure choices. Keeping track of current discussions about stricter liability of the manufacturer will be interesting, but globally, there will always be cheaper, less secure options. We need to keep thinking about DDoS mitigations, too.



Balthasar lives in Berlin where he pursues a Masters in IT-Systems engineering while working at SRLabs. He is fascinated by a world populated by "smart" devices that turn out to be as smart as a slice of bread. After the DDoS on[Brian Krebs](), he got curious about additional ways to disturb the global Internet matrix.



Fabian studied IT-Systems Engineering at HPI in Potsdam, but was always more curious about taking such systems apart. He now works as a Security Researcher and Consultant at Berlin-based hacker collective SRLabs. Fabians previous talks include hacking payment systems at 32c3 and travel systems at HEUREKA.

Posted in:Conference,Internet,Security | Tagged:Botnet,DDoS,DeepSec,IoT,Network,Research,Talk | With 0 comments