

01.10.18

Har du styr på sikkerheden i dine IoT-enheder? **IoT botnets**



www.pwc.com/digital

IoT botnet

Et IoT botnet er et netværk af ”robotter” i form af internet forbundet IoT-enheder der er blevet inficeret af samme malware og hermed kan fjernkontrolleres.

IoT botnets

2008 2010

HYDRA

TSUNAMI

PSYBOT

2009

2014 2016

GAFGYT

MIRAI

TROJAN.LINUX.PNSCAN

BRICKERBOT

2015 2017

01

Mirai

Mirai – IoT botnet

Mirai DDoS-angreb

- Krebs on security, ~24.000 enheder, >600 Gbps [1]
- OVH, >145.000 enheder, ~1 Tbps [2]
- Dyn, ~100.000 enheder, ~1 Tbps[3]

Overordnede funktionalitet [4]

- Skanning af internettet (telnet port 23 og 2323)
- Hardcodede blacklist af IP-adresser
- Brute-force af credentials
- Asynkron inficering af enheder



6 måneder senere

Hajime

- Bygget på samme fundament som Mirai
- Monitorering af trafik og indlæring af adfærd for at kunne efterligne denne
 - Fjernelse af firewall regler

1 år senere

Reaper / IoTroop

- Indeholder kode fra Mirai
- Udnyttelse af minimum ni kendte sårbarheder

02

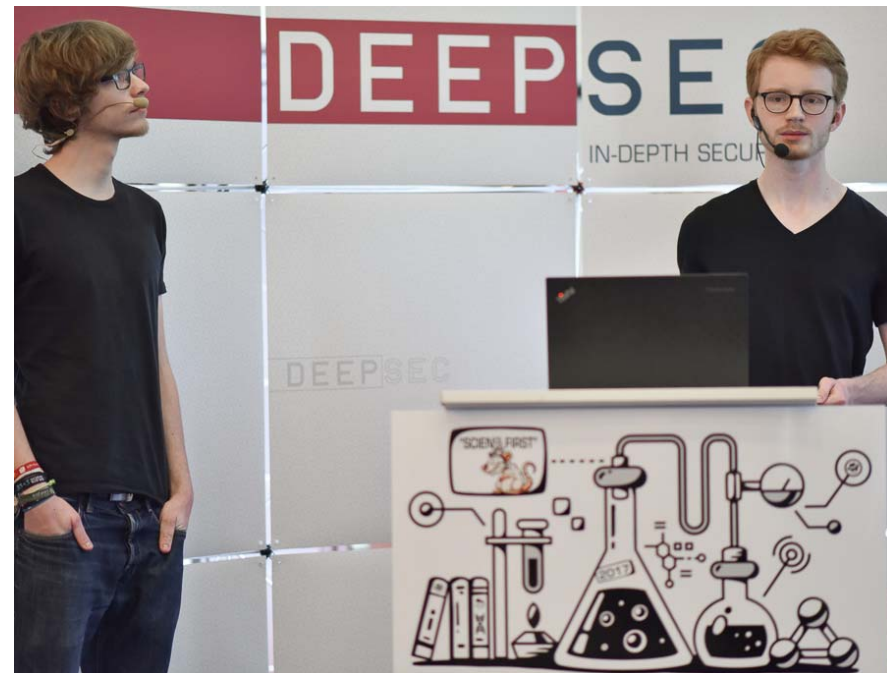
Næste generation

Security Research Labs – Next-gen Mirai

Cloud services eksponere private IP-kamera

- Liste af aktive enheder
 - Videoipcamera: 140.741 enheder
 - Cloudlinks: 3.277.280 enheder
- Default password
 - Videoipcamera: 63.000+ enheder (888888)
 - Cloudlinks: 700.000+ enheder (123)
- Remote code execution (Videoipcamera)
 - DNS server ændret for at omdirigere enhedernes opdateringsforespørgelser
 - Initierer en firmware opdatering
 - Leverer ondsindet firmware

Balthasar Martin, Fabian Bräunlein [5]



Tak!

- [1] <https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/>
- [2] <https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac>
- [3] <https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>
- [4] <https://jhalderm.com/pub/papers/mirai-sec17.pdf>
- [5] <https://srlabs.de/bites/cloud-cameras/>

© 2016 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.