KØBENHAVNS UNIVERSITET

Ukendte trusler i universiteternes netværkstrafik

Bo Bendix, Koncern it, Core-services
Københavns Universitet

Et godt tilbud

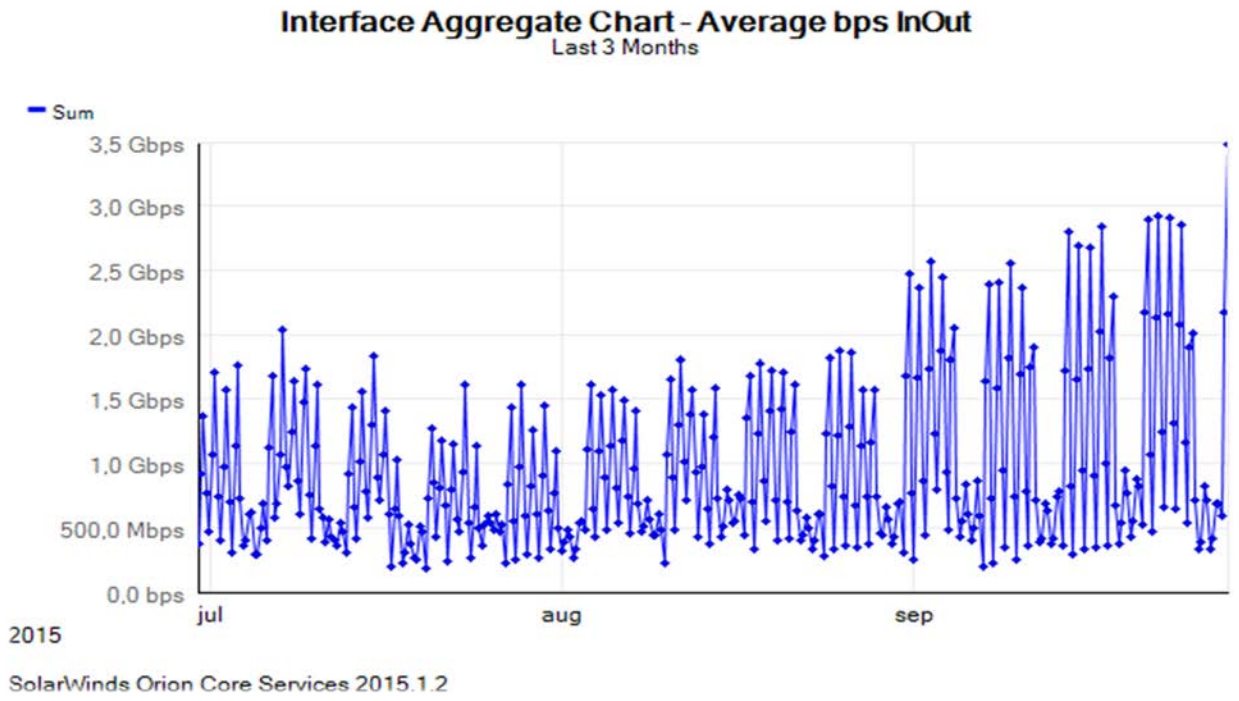
Formål: At identificere ukendte trusler der rammer brugere og systemer.

KPMG
cutting through complexity™

FireEye

Tilbud: KPMG og FireEye undersøgte i februar 2015 18 danske private og offentlige virksomheder – ganske gratis.

Hvordan?



FireEye satte en boks på vores primære 10G link ud/ind og modtog en mirrow af al trafik der løb igennem

Hvad så vi?

Computer Alerts

99,2%

0,5%

0,2%

Mobile Alerts

7%

93%

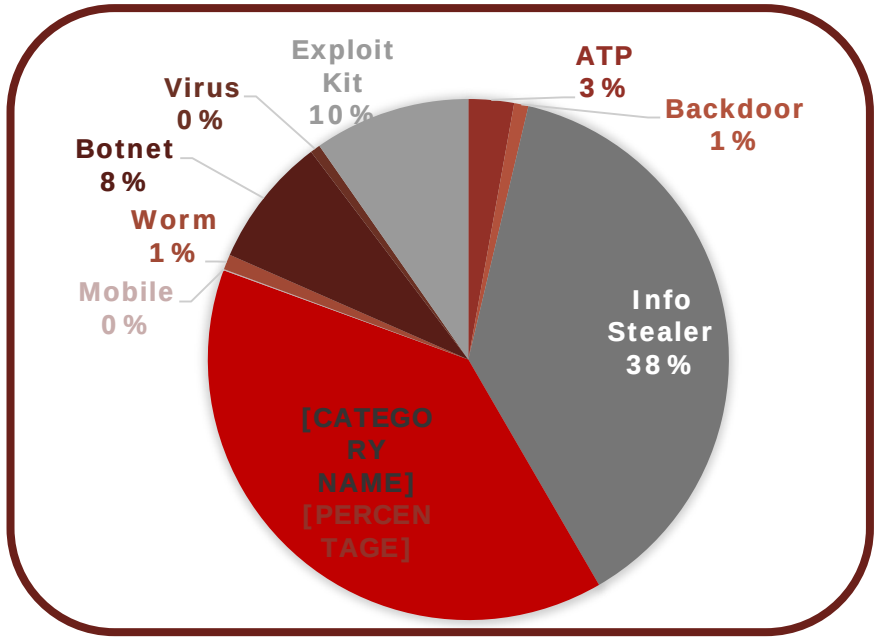
Hvad så vi?

KU:
Indgående : 13 %
Udgående: mange %

Malicious event summary

- Inbound malicious events observed: 31355
- Outbound malicious events observed: 87647

- Threat Alerts Summarized in Categories
  - APT: 3356
  - Backdoor: 1057
  - Info Stealer: 45120
  - Trojan: 46318
  - Mobile: 86
  - Worm: 1122
  - Botnet: 9639
  - Virus: 746
  - Exploit Kit: 11528



Hvad ved vi?

Der blev detekteret multiple Exploits Kits

Kompromitterede enheder kommunikerede med C & C servere

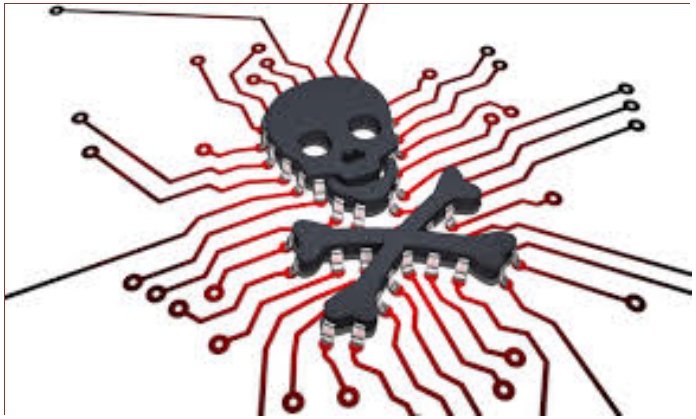
Hvad ved vi?

Malware blev sendt til brugerne via ”phishing” mail – og afviklet

En enkelt ”APT” blev modtaget og ”implementeret”

Hvad ved vi?

- Uautoriseret aktivitet
- Brug af enheder (RAT) placeret på KU



Hvad gør KU så ved det?

Tager det ganske roligt☺
Det er jo kun eduroam brugere som bliver ramt

Mange udgående kald i forhold til indgående indikerer at klienterne er inficeret udenfor vores ”beskyttelse”

Hvad gør KU så ved det?

En større kilde til de modagne trusler, e-mail, har fået ekstra sikkerhed

Tager undersøgelsen med i en større sikkerhedssatsning – for at blive mere klar… (vi mener det er nødvendigt..)

Vi er ikke alene bag vores firewall…