F-Secure

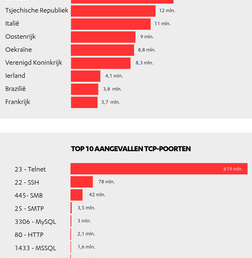
# HET BEDREIGINGSLANDSCHAP H2 2018

Door ons wereldwijd honeypot-netwerk gedetecteerd aanvalsverkeer juli t/m december 2018

## *Een verviervoudiging van het aanvals- en verkenningsverkeer*

### TOTALE AANTAL AANVALLEN OP HONEYPOTS PER PERIODE


### BELANGRIJKSTE LANDEN VAN HERKOMST




Het meeste aanvalsverkeer was afkomstig van IP-adressen in de VS. Verkeer uit Rusland kwam op de tweede plaats.

### BELANGRIJKSTE LANDEN VAN BESTEMMING


### TOP 10 AANGEVALLEN TCP-POORTEN


Met malware besmette IoT-apparaten, ook wel 'thingbots' genoemd, waren verantwoordelijk voor het meeste Telnet-verkeer.

## *Misbruik van webservers is ook een belangrijke aanvalstechniek*

### SERVERS EN SERVICES


## POGINGEN TOT MISBRUIK VAN AANMELDINGSGEGEVENS VOOR AANVALLEN

| TOP 10 GEBRUIKTE GEBRUIKERSNAMEN | TOP 10 GEBRUIKTE WACHTWOORDEN |
|---|---|
| root | admin |
| admin | vizxv |
| shell\x00 | root |
| guest | default |
| default | 123456 |
| shell | xc3511 |
| enable\x00 | 12345 |
| supervisor | taZz@23495859 |
| support | 1001chin |
| user | 1234 |

Maak nooit gebruik van gebruikersnamen en wachtwoorden die op deze lijst voorkomen!

## DOOR BEDRIJVEN GEDETECTEERDE AANVALLEN

Gebaseerd op een enquête onder bedrijven in 12 landen

### DETECTIE VAN AANVALLEN IN HET AFGELOPEN JAAR




Sectoren met hoogstwaarschijnlijk 5 of meer aanvalsdetecties: Financiële sector, ICT-sector

Sectoren met de minste aanvalsdetecties: Gezondheidszorg, productie-industrie

Iets minder dan een derde van alle respondenten beschikt over een oplossing voor detectie en incidentrespons

*Bron: Een enquête onder 3.350 IT-beslissers, -influencers en -managers in 12 landen

## BEVEILIG UW BEDRIJFSASSETS

**Beperk uw aanvalsoppervlak.** Reduceer waar mogelijk de complexiteit van uw netwerken, software en hardware. Zorg ervoor dat u precies weet welke systemen en services er binnen uw organisatie worden gebruikt en deactiveer alles wat u niet nodig hebt.

**Betrek uw medewerkers.** Licht uw personeel voor over cybersecurity en de toepassing van best practices op dit gebied. Zorg voor processen en procedures die zij gemakkelijk kunnen opvolgen.

**Gebruik gelaagde beveiliging.** Hanteer een gelaagde beveiligingsaanpak die een combinatie omvat van voorspellende functionaliteit (predict), preventieve mechanismen (prevent), detectiemogelijkheden (detect) en technologie voor incidentrespons (respond).

F-Secure