Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices

Nieuwsbericht | 10-06-2024 | 12:00

Eerder dit jaar heeft het NCSC samen met de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een rapport gepubliceerd over de geavanceerde COATHANGER-malware gericht op FortiGate-systemen. Sindsdien heeft de MIVD nader onderzoek gedaan en is gebleken dat de Chinese cyberspionagecampagne veel omvangrijker blijkt te zijn dan eerder bekend. Het NCSC vraagt daarom extra aandacht voor deze campagne en het misbruik van kwetsbaarheden in edge devices. Hiervoor heeft het NCSC een kennisproduct opgesteld met aanvullende informatie over edge devices, bijbehorende uitdagingen en te nemen maatregelen.

De bredere COATHANGER-campagne

Sinds de publicatie in februari heeft de MIVD verder onderzoek gedaan naar de bredere Chinese cyberspionagecampagne. Hieruit is naar voren gekomen dat de statelijke actor zowel in 2022 als in 2023 binnen enkele maanden toegang heeft verkregen tot ten minste 20.000 FortiGate-systemen wereldwijd middels de kwetsbaarheid met het kenmerk CVE-2022-42475. Verder toont onderzoek aan dat de statelijke actor achter deze campagne minimaal twee maanden voordat Fortinet de kwetsbaarheid bekend maakte, al op de hoogte was van deze kwetsbaarheid in FortiGate-systemen. Tijdens deze zogeheten ‘zero-day’ periode, infecteerde de actor alleen al 14.000 apparaten. Onder doelwitten zijn onder meer tientallen (westerse) overheden, internationale organisaties en een groot aantal bedrijven binnen de defensie-industrie.

De statelijke actor installeerde bij relevante doelwitten op een later moment malware. Zo kreeg de statelijke actor permanente toegang tot de systemen. Ook als een slachtoffer beveiligingsupdates van

FortiGate installeert, blijft de statelijke actor deze toegang houden.

Het is niet bekend bij hoeveel slachtoffers daadwerkelijk malware is geïnstalleerd. De Nederlandse inlichtingendiensten en het NCSC achten het waarschijnlijk dat de statelijke actor in potentie bij honderden slachtoffers wereldwijd zijn toegang uit kon breiden en aanvullende acties uit heeft kunnen voeren zoals het stelen van gegevens.

Zelfs met het technische rapport over de COATHANGER-malware zijn infecties van de actor lastig te identificeren en te verwijderen. Het NCSC en de Nederlandse inlichtingendiensten stellen daarom dat het waarschijnlijk is dat de statelijke actor op dit moment nog steeds toegang heeft tot systemen van een significant aantal slachtoffers.

Mitigerende maatregelen bij het gebruik van edge devices

Het NCSC en de Nederlandse inlichtingendiensten zien al langer een trend dat kwetsbaarheden in publiek benaderbare edge devices zoals firewalls, VPN-servers, routers en e-mailserververs worden misbruikt. Vanwege de uitdagingen op het gebied van beveiliging van edge devices zijn deze apparaten een geliefd doelwit voor kwaadwillenden. Edge devices bevinden zich aan de rand van het IT-netwerk en hebben geregeld een directe verbinding met het internet. Daarnaast worden deze apparaten vaak niet ondersteund door Endpoint Detection and Response (EDR) oplossingen.

Initiële compromittering van een IT-netwerk is moeilijk te voorkomen als de kwaadwillende hierbij gebruik maakt van een zero-day. Daarom is het van belang dat organisaties het ‘assume breach’-principe hanteren. Dit principe hanteert dat een succesvolle digitale aanval al heeft plaatsgevonden of binnenkort gaat plaatsvinden. Op basis hiervan worden maatregelen genomen om de schade en impact te beperken. Denk hierbij aan het nemen van mitigerende maatregelen op het gebied van segmentering, detectie, incident response plannen en forensic readiness.

Het NCSC kennisproduct ‘Omgaan met edge devices’ beschrijft verdere uitdagingen en digitale dreigingen bij het gebruik van edge devices en biedt per uitdaging concreet handelingsperspectief voor organisaties.

Kennisproduct 'Omgaan met edge devices'

- **Factsheet Omgaan met edge devices**

  Hedendaagse organisaties maken vaak gebruik van edge devices. Deze systemen bevinden zich aan de rand van het netwerk en bestaan ...

  Factsheet | 10-06-2024