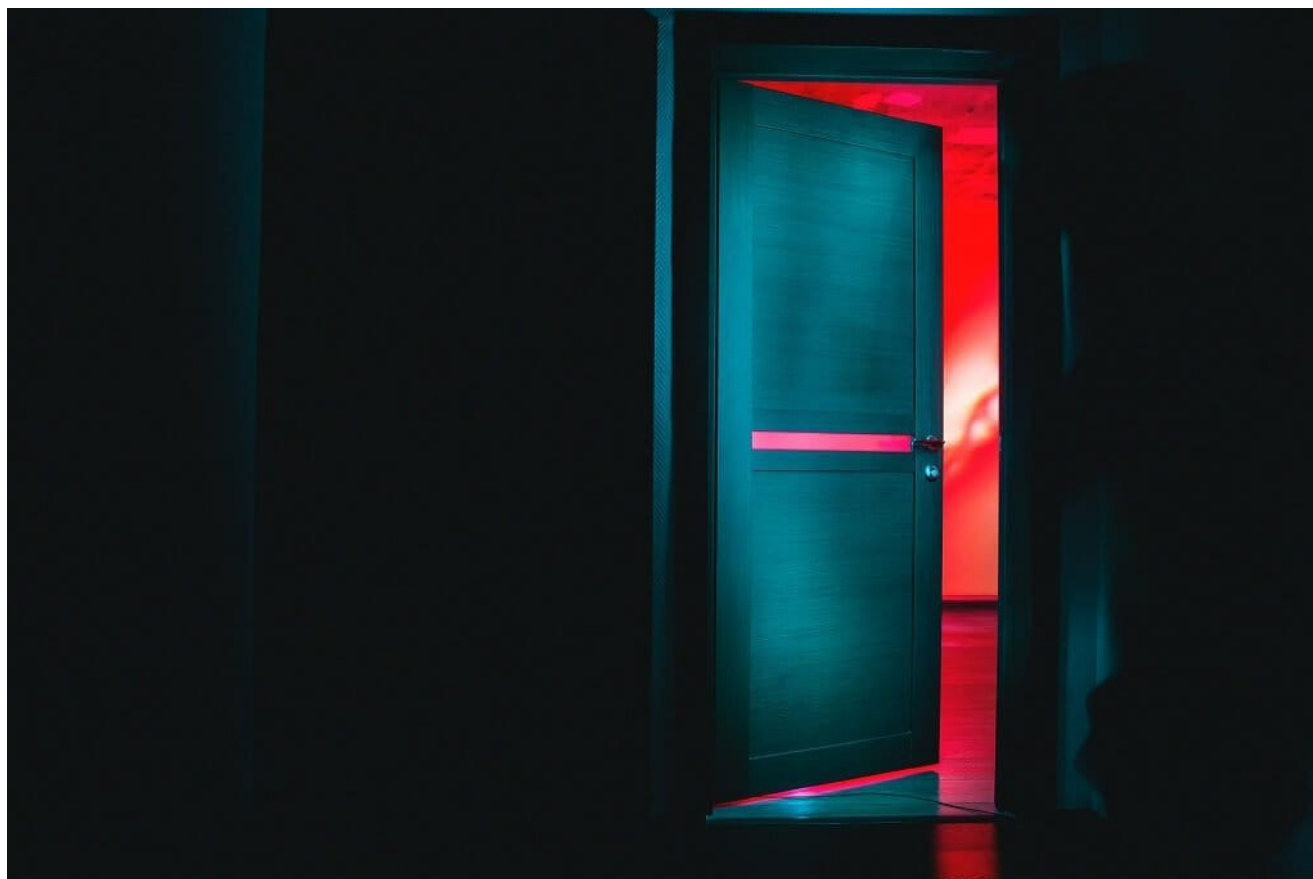


PRESSEMEDDELELSE

PRESSEMEDDELELSE - Hackergruppen FIN8 er tilbage med en endnu farligere trussel

Pressemeddelelse · Udgivelse og medieindhold



Cybersikkerhedsfirmaet Bitdefender har fundet beviser for, at hackergruppen FIN8 igen er begyndt at angribe organisationer efter længere tids dvale. Nu med en mere sofistikeret udgave af deres bagdør, BADHATCH.

FIN8 og deres malware-bagdør, BADHATCH, er atter tilbage. Bitdefender har observeret, at hackergruppen har udviklet nye versioner af BADHATCH siden 2019. Blandt de nye egenskaber, bagdøren nu har fået, er blandt andet muligheden for at tage billeder af offerets skærm, udføre filløse eksekveringer og etablere proxy tunneller. Derudover bruger BADHATCH TLS kryptering, der gør det sværere for sikkerhedsløsninger at opfange de powershell kommandoer, som malwaren bruger.

Den avancerede bagdør gør det muligt for FIN8 at indsamle informationer om offerets netværk og inficere andre computere på netværket uden at blive opdaget.

FIN8 er en økonomisk motiveret hackergruppe, der har været aktive siden 2016. De er kendt for at iværksætte en lang række skræddersyede angreb, fra *spear phishing*-kampagner til *zero-day* sårbarheder i Windows. Angrebene er rettet mod detailvirksomheder, hotel- og restaurationsbranchen, samt underholdningsbranchen, med det formål at stjæle betalingskortoplysninger fra POS (*Point of Sale*) kassesystemer.

BADHATCH blev første gang dokumenteret i 2019 af GIGAMON, men nu er FIN8 altså vendt tilbage med en styrket version. Hackergruppen er kendt for at tage lange pauser, hvor de forbedrer deres taktik, teknikker og procedurer med henblik på at opnå bedre resultater.

Bitdefender har siden FIN8's tilbagekomst sidste år dokumenteret angreb på ofre i blandt andet USA, Canada og Italien og opfordrer derfor organisationer til at være på vagt og holde øje med kendte indikatorer på kompromittering.

Bitdefender har en række råd til, hvad man kan gøre for at beskytte sig bedre mod økonomisk motiverede hackere som FIN8:

- Adskil POS-netværket fra de netværk, som ansatte og gæster bruger.
- Træn de ansatte i at være mere opmærksomme på cybersikkerhed, som kan hjælpe dem med at spotte phishing-mails. Og indstil e-mail indbakkens sikkerhedsløsning til automatisk at kassere farlige eller suspekte vedhæftninger.
- Integrér trusselsefterretninger som en del af den eksisterende SIEM (*Security Information and Event Management*) eller sikkerhedskontroller for at få relevante indikatorer på kompromittering.
- Små og mellemstore organisationer der ikke har et dedikeret IT-sikkerhedsteam bør overveje at outsource opgaven til professionelle MDR (*Managed Detection and Response*) udbydere.

Du kan finde en teknisk gennemgang af BADHATCH og de nye angreb her:

<https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf>

Kilde / Logo / Foto: Bitdefender

Online: <https://pressemeddelelse.dk/pressemeddelelser/pressemeddelelse-hackergruppen-fin8-er-tilbage-med-en-endnu-farligere-trussel/>

Pressemeddelelsen er videreformidlet af Pressemeddelelse.dk. Pressemeddelelse.dk er ikke ansvarlig for indholdet. Spørgsmål til indholdet rettes til Bitdefender.