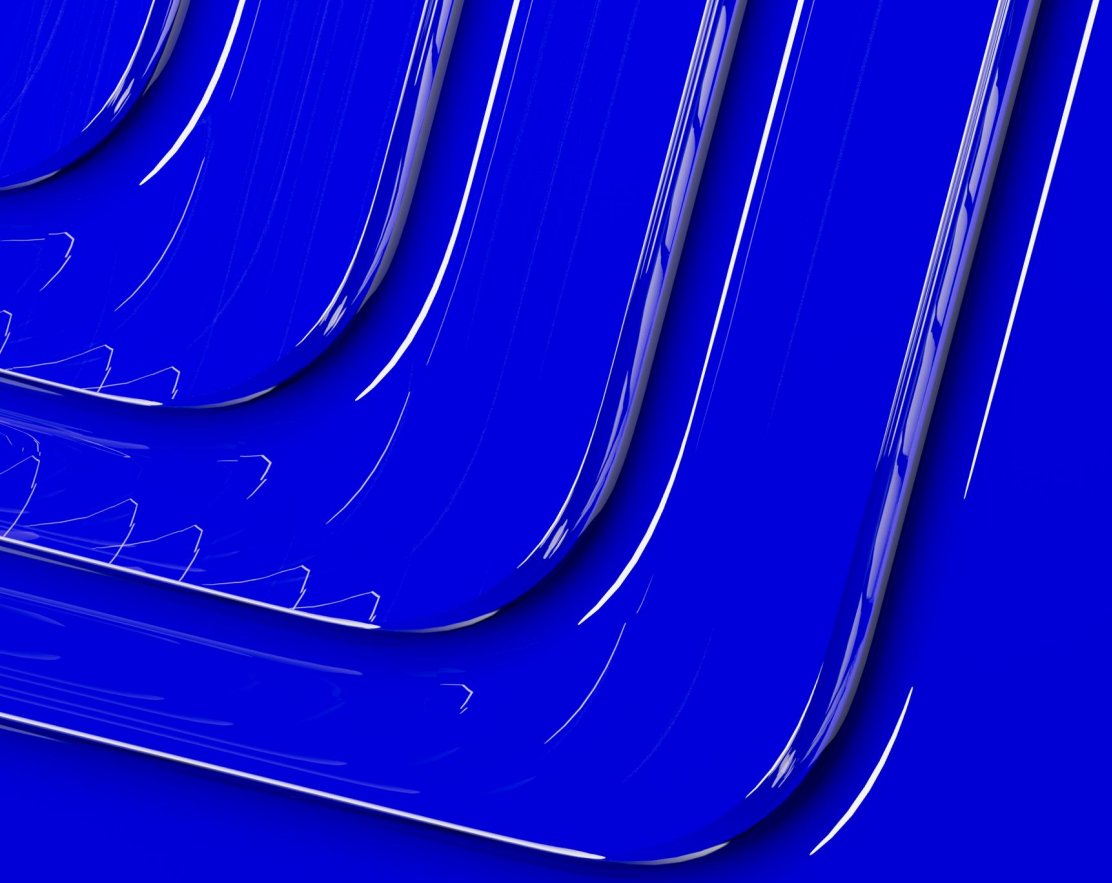
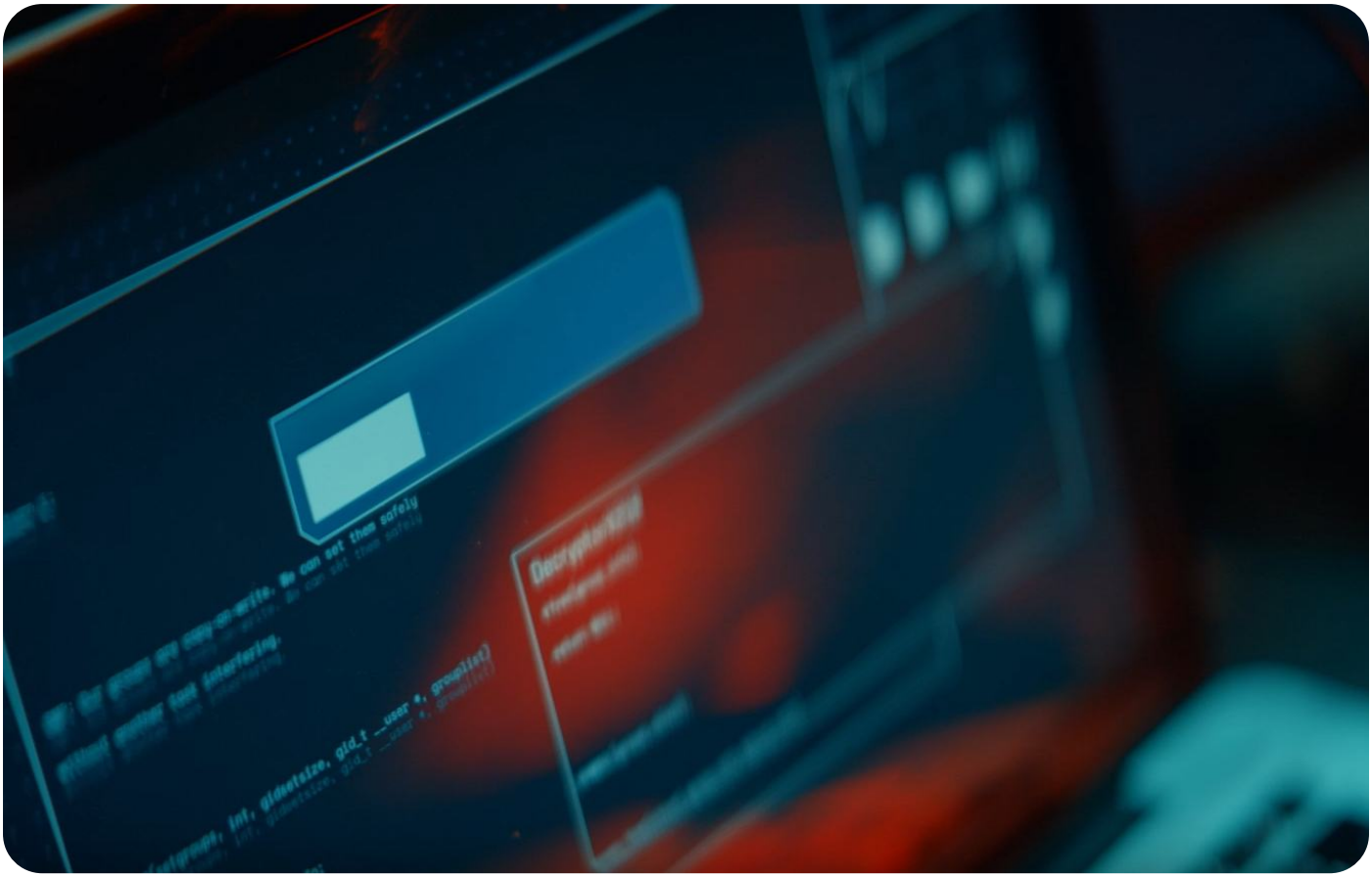


TDC Erhverv
Se fremad

TDC Erhverv Sikkerhedsrapporten Q3 2024

Phishing-boom og feriestemning



Q3 var generelt et roligere kvartal sammenlignet med Q1 og Q2, når vi måler på antallet af blokeringer. Mens vi i Q2 registrerede næsten 5,5 millioner blokeringer udført af TDC Erhvervs Internetfilter, nåede vi i Q3 kun op på omkring 3 millioner. Dette indikerer et Danmark, hvor mange virksomheder har haft ferielukket, og hvor enhederne simpelthen har været slukkede. Færre klik betyder færre registrerede angreb — så enkelt er det.

Vi observerede en stigning i mængden af malware, et fald i command & control-aktiviteter og en markant udvikling i phishing-angreb sammenlignet med Q2. Sommerens store begivenheder som EM i fodbold og OL ser ud til at have bidraget til denne stigning i phishing-angreb. Sådanne events er ofte en katalysator for hackere til at bruge phishing som metode til at narre betalingsoplysninger og data fra brugerne.

Dyk ned i tallene, tendenserne og trusselstyperne, der prægede Q3, i vores Sikkerhedsrapport. Her stiller vi også helt skarpt på en klassisk trusselstype, der desværre ser ud til at få ny vind i sejlene — nu med hjælp fra AI — nemlig phishing. Men først tager vi et kig på tallene for Q3.

Q3 i talhøjde

Vi kan se tilbage på et kvartal, hvor antallet af blokeringer igen faldt ganske markant. Hvilket nok primært hænger sammen med sommerferie.

3 mio.

Vi nåede op på knap 3 mio. blokeringer **– 2.912.973 i alt.**

I gennemsnit betyder det, at Internfilter blokerede **2,2 domæner for hver eneste kunde** – hver dag.

Top 3 trusler i Q3

67,6 % Malware

Hvad er Malware?

Er alle former for ondsindet software designet til at skade enheder og systemer. 51,3 % i Q2.

11,3% C&C

Hvad er C&C?

Er cyberangreb, der vil styre og kontrollere de devices, de har inficeret med malware eller ondsindet software. 35,2 % i Q2.

17,3 % phishing

Ny i top 3

Hvad er phishing?

Er falske e-mails, beskeder eller websider, der ligner dem fra troværdige kilder, som vil narre adgangskoder, kreditkortnumre og personlig info ud af brugeren.

Som vi slog an i Sikkerhedsrapporten for Q2 er phishing stadig et meget potent værktøj for cyberkriminelle, hvilket en placering i top 3 understreger. Senere her i rapporten stiller vi helt skarpt på phishing, som nu tilsat AI ser ud til at være mere potent og farligere end nogensinde.

Deep dive på to vinkler af phishing

Hvert kvartal ser vi i Sikkerhedsrapporten nærmere på trusler og angreb, der har fanget vores opmærksomhed ekstra meget, og Q3er ingen undtagelse. Denne gang dykker vi ned i phishing:

Phishing, der vil stjæle kreditoplysninger

Vi har alle været udsat for denne type phishing, hvor vi bliver bedt om at klikke på et link i en e-mail, der ved første øjekast ser ægte ud med logo og design. Klikker man, lander man på et falsk website, der umiddelbart ser legitimt ud. Her skal man indtaste sine kreditkortoplysninger, og hvis man gør det, kan det hurtigt blive en dyr fornøjelse for både brugeren og virksomheden.

Phishing, der vil installere malware

En anden metode er phishing, der forsøger at få os til at opdatere software via hjemmesider som ligner Microsoft eller Chrome. Klikker man på download, begynder en falsk opdatering, som skjult installerer malware på vores enhed for at overvåge og optage vores aktiviteter. Denne type phishing-angreb udgør alvorlige sikkerhedstrusler får både brugeren og virksomheden, da de stjålne data kan bruges til yderligere svindel eller identitetstyveri.

Tendens:

Næste generations phishing er optimeret af AI

Phishing-angreb bliver stadig mere sofistikerede, og med den stigende brug af AI ser de ud til at tage et kvantespring fremad. Med AI kan de cyberkriminelle skabe langt mere overbevisende og personlige beskeder og indhold, der er sværere at skelne fra legitim kommunikation. Det ser så ægte ud, at det stiller større krav om mere effektiv it-sikkerhed og bedre digital adfærd hos den enkelte.

Ved hjælp af AI-algoritmer kan de cyberkriminelle automatisk analysere store datamængder og tilpasse deres angreb baseret på individuelle præferencer og adfærdsmønstre. Det gør deres forsøg langt mere målrettede og effektive. Derudover kan AI bruges til at efterligne sproget og tonen fra velkendte virksomheder eller personer, hvilket gør phishing-beskeder endnu mere troværdige.

Efterhånden som teknologien udvikler sig, forventer vi, at AI-drevet phishing vil være endnu vanskeligere at opdage og bekæmpe. Det er derfor vigtigere end nogensinde at være opmærksom og forberedt på denne nye generation af cybertrusler.

Vær ekstra meget på vagt i Q4

Black Friday og julen står for døren, hvilket er højtider for hackere. Så vi forudser, at phishing, når vi ser tilbage på Q4, vil fylde endnu mere i trusselsbilledet. Tag jer i agt for den nye generation af phishing. Her er nogle sikkerhedsprincipper, der er gode at huske på, så hackerne ikke får fisket noget af værdi:

Vær skeptisk overfor ukendte afsendere

Åbn aldrig e-mails, links eller vedhæftede filer fra afsendere, du ikke kender eller har mistanke om kan være falske.

Tjek URL'en nøje

Phishing-websites efterligner ofte legitime sider. Tjek altid webadressen for fejl eller usædvanlige tegn.

Opdater din software regelmæssigt

Sørg for, at dit operativsystem, antivirus-program og software er opdateret med de nyeste sikkerhedsopdateringer.

Brug spamfiltre

De fleste e-mail-tjenester har indbyggede spamfiltre, der kan hjælpe med at filtrere mistænkelige e-mails fra. Sørg for, at dit spamfilter er aktiveret og opdateret.

Del aldrig personlig info unødigt

Del aldrig dine personlige oplysninger, som passwords, kreditkortnumre eller følsomme data via e-mail eller tekstbeskeder.

Klik ikke på mistænkelige links

Hvis du modtager en e-mail med et link, så undgå at klikke direkte på det. Hold musen over linket for at se, hvor det fører hen, eller indtast webadressen manuelt i din browser.

Vær på vagt overfor hastværk og pres

Phishing-angreb forsøger ofte at skabe en følelse af hastværk eller panik. Tænk dig om, før du reagerer på beskeder, der kræver øjeblikkelig handling eller truer med alvorlige konsekvenser.

TDC Erhverv
Se fremad

Er I klar til et cyberangreb?

Ja? Så hører I faktisk til et mindretal. I vores rapport "Er jeres virksomhed klar til i morgen" svarer kun 1 ud af 5 virksomheder nemlig, at de har en plan, hvor alle medarbejdere ved, hvad de skal gøre, hvis virksomheden udsættes for et cyberangreb. Hent hele rapporten **her.**

Læs mere om
TDC Erhverv InternetFilter på
www.tdc.dk/produkter/internetfilter