TDC Erhverv

TDC Erhverv Sikkerhedsrapport Q1 2026

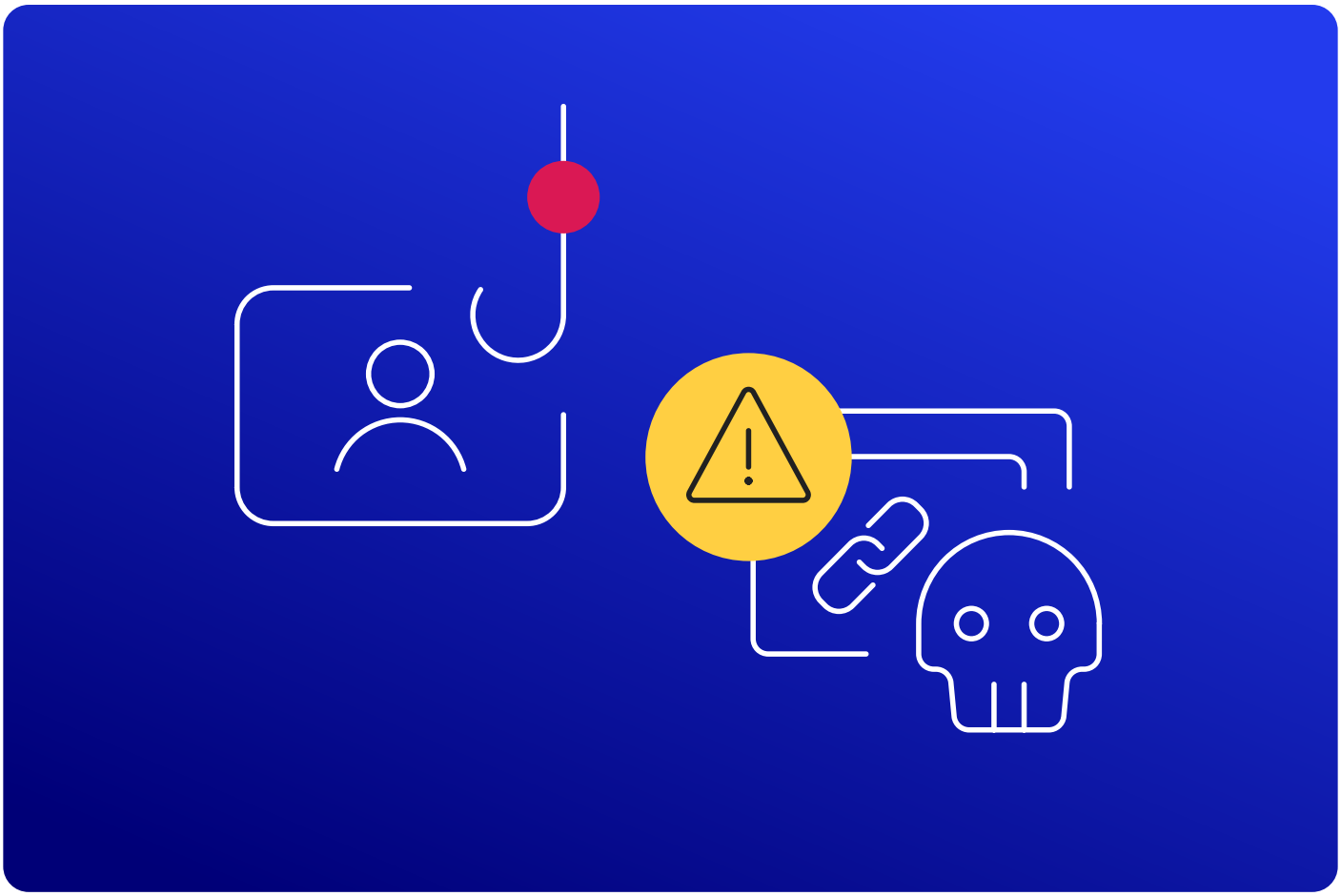
Q1, kort fortalt

Q1 2026 viser et trusselsbillede, hvor cyberangreb rammer bredt på tværs af virksomheder og offentlige institutioner i Danmark – og hvor kompromitteringer ofte er karakteriseret af diskrete metoder. I løbet af kvartalet observerede TDC Erhverv Cyber Threat Intelligence **1.681** hændelser, der indikerer kompromittering med malware blandt virksomheder og organisationer i Danmark.

Rapporten peger særligt på tre udviklinger inden for cybertrusler i Danmark:

- Informationsstjælende malware som RisePro, AsyncRat og XWorm spiller en markant rolle i trusselsbilledet. Angrebene handler i høj grad om at stjæle loginoplysninger, data og adgang til systemer.
- Små og mellemstore virksomheder er blandt de mest udsatte. Virksomheder med 1–100 medarbejdere står samlet for 54,8 % af de observerede hændelser i Q1. Det understreger, at cybertrusler ikke kun er en udfordring for store organisationer.
- Offentlige institutioner og samfundsvigtige funktioner er under et særligt pres. Kommuner er de mest ramte i Q1 2026 med 20,6 % af de observerede hændelser. Samtidig har TDC Erhverv Security Operations Center observeret en stigende aktivitet af DDoS-angreb mod domæner tilknyttet danske offentlige institutioner.

På tværs af rapportens analyser står én ting klart: Moderne cyberangreb handler ikke nødvendigvis om spektakulære nedbrud, men om hurtig adgang til data, identiteter og systemer. Derfor bliver evnen til hurtigt at opdage kompromitteringer og reagere effektivt stadig vigtigere for virksomheder og organisationer i Danmark.



Datagrundlaget bag rapporten

I TDC Erhverv leverer vi internettrafik til små, mellemstore og store virksomheder samt myndigheder og offentlige institutioner i Danmark. Det giver os adgang til unik metadata, som vi analyserer i realtid og omsætter til et repræsentativt overblik over det aktuelle trusselsbillede på tværs af bl.a. brancher, virksomhedstyper og geografiske områder[1].

Metadataen bygger på mere end 100 milliarder anonymiserede flowdatapunkter for den trafik, der passerer gennem vores netværk fra og til kunderne. Et flowdatapunkt er et registreret stykke metadata om netværkstrafik – altså information om, at en digital forbindelse har fundet sted, uden indsigt i selve indholdet. Det kan for eksempel være oplysninger om, hvilke enheder der kommunikerer, hvornår kommunikationen sker, hvor længe den varer, og hvilke protokoller eller tjenester der bruges.

Et flow i netværkstrafik kan altså forstås som en "samtale" mellem to enheder. Det beskriver en gruppe datapakker, der hører sammen, fordi de har samme kilde, destination, porte og protokol. For eksempel vil en computers eller smartphones hentning af en hjemmeside fra en server blive registreret som ét flow. Alt dette sammenholdes og analyseres i enorm skala med kunstig intelligens og avancerede analyser – bl.a. ved hjælp af Danmarks nationale AI-supercomputer Gefion. Resultatet er dansk trusselsindsigt, som giver os og vores kunder et unikt forspring i arbejdet mod cyberangreb.

[1]Datagrundlaget er analyseret ud fra gældende indikatorer på tidspunktet for udarbejdelsen. Resultaterne er derfor med forbehold for ændringer, hvis ny information eller nye efterretninger fremkommer.

Q1 2026 i tal

1.681

Hændelser blandt virksomheder og organisationer i Danmark, der indikerer kompromittering med malware i Q1 2026.

I Q1 2026 observerede TDC Erhverv Cyber Threat Intelligence 1.681 hændelser i internettrafikken, der indikerer, at de berørte virksomheder sandsynligvis har været kompromitteret med malware. Når blot ét vellykket angreb kan være nok til at skabe store driftsmæssige og økonomiske konsekvenser, understreger hændelserne alvoren i det aktuelle trusselsbillede.

I rapporten *"Er jeres virksomhed klar til i morgen?"*, udarbejdet sammen med analyseinstituttet Ipsos i 2026, har vi kortlagt de økonomiske konsekvenser af cyberangreb. Her estimeres omkostningerne ved blot én dags nedlukning efter et vellykket cyberangreb til **70.000 kr.** for små virksomheder, **190.000 kr.** for mellemstore virksomheder og **500.000 kr.** for store virksomheder.

Top 5 mest udbredte malwarefamilier

1. AsyncRat
2. XWorm
3. XenoRat
4. Remcos
5. RisePro

Top 5 mest angrebne brancher

1. Kommuner (20,6 %)
2. Telekommunikation (12,2 %)
3. Tekstilproduktion og -efterbehandling (8,5 %)
4. Offentlig forvaltning og administration (Forsvaret ikke inkluderet) (7,3 %)
5. Computerprogrammering, it-infra-struktur og it-konsulentbistand (4,8 %)

Fordeling af observerede hændelser efter virksomhedsstørrelse:

Virksomheder med 1-10 medarbejdere: 25,4 %

Virksomheder med 10-100 medarbejdere: 29,4%

Virksomheder med 100-400 medarbejdere: 11,4%

Virksomheder med 400-1.000 medarbejdere: 11,3%

Virksomheder med 1.000+ medarbejdere: 22,5 %

Størstedelen af hændelser er observeret blandt **små og mellemstore virksomheder**

Mange forbinder stadig cyberangreb med store internationale virksomheder, kritisk infrastruktur og organisationer med særligt værdifulde data. Men trusselsbilledet ser anderledes ud i praksis. Nutidens cyberangreb handler nemlig ikke kun om størrelse, men også om sikkerhedsniveau og muligheden for at bruge én virksomhed som adgangsvej til en anden. Derfor rammes både små, mellemstore og store virksomheder i dag af digitale trusler – blot på forskellige måder.

I Q1 2026 har TDC Erhverv Cyber Threat Intelligence identificeret 1.681 hændelser på tværs af virksomheder i Danmark. Analysen viser, at små og mellemstore virksomheder fortsat fylder markant i trusselsbilledet. Samlet står virksomheder med 1–100 ansatte for 54,8 % af de observerede hændelser. Til sammenligning udgør virksomheder med over 1.000 ansatte 22,5 %. Det understreger, at cybersikkerhed ikke kun er en problemstilling for store virksomheder.

SMV'er er attraktive mål

Små og mellemstore virksomheder har typisk færre ressourcer til it-sikkerhed, mindre specialiserede sikkerhedsteams og lavere modenhed i deres sikkerhedsarbejde. Samtidig er de digitale værktøjer til at udføre angreb blevet mere tilgængelige. Det betyder, at ondsindede aktører i dag kan gennemføre angreb i stor skala uden nødvendigvis at have avancerede ressourcer eller kapaciteter.

Blandt de 1.681 observerede hændelser i Q1 ser vi særligt en overvægt af offentligt tilgængelige infostealers, der rammer mindre virksomheder. En infostealer er malware designet til at stjæle informationer fra kompromitterede enheder, fx adgangskoder, cookies, browserdata, loginoplysninger eller oplysninger fra e-mail- og samarbejdsværktøjer.

Samtidig er mange mindre virksomheder i dag tæt integreret med større kunder, leverandører og samarbejdspartnere. Derfor kan kompromittering af en mindre virksomhed også fungere som adgangsvej til større og mere strategisk interessante mål længere inde i værdikæden.

Målet er ikke altid den største, men den nemmeste

SMV'er er altså i stigende grad blevet en del af det bredere trusselsbillede og kan ikke længere betragte cybersikkerhed som noget, der primært vedrører de store virksomheder. Det er blevet en grundlæggende del af det at drive virksomhed – uanset størrelse – og derfor bør alle sikre:

- Regelmæssig backup
- Løbende opdatering og vedligeholdelse af systemer
- Træning af medarbejdere i sikker digital adfærd
- Sikkerhedsovervågning af netværk og endpoints for hurtig detektion af angreb
- Klare procedurer for håndtering af sikkerhedshændelser

Kommuner er mest ramt i Q1 2026

Ser man på fordelingen af angreb blandt brancher, er kommuner den mest ramte sektor i Q1 2026 med 20,6 % af de registrerede hændelser.

Det er dog væsentligt at bemærke, at en del af hændelserne sandsynligvis stammer fra skolenetværk og andre ikke-overvågede miljøer. I disse tilfælde ser vi en overvægt af offentligt tilgængelig malware og infostealers, som typisk rammer bredt og mindre beskyttede systemer. Det ændrer dog ikke ved, at kommunerne samlet set udgør en stor og kompleks digital flade med mange brugere, enheder og systemer – ofte med varierende sikkerhedsniveauer på tværs af organisationerne.

XWorm og kontrol over kompromitterede enheder

Ser man isoleret på kommunerne, relaterer ca. 25 % af de registrerede hændelser sig til XWorm-malware. XWorm er en avanceret Remote Access Trojan (RAT), der giver angribere omfattende kontrol over kompromitterede systemer.

Malwaren understøtter en bred vifte af funktioner, herunder datatyveri, systemovervågning og fjernstyring. Samtidig kan kompromitterede enheder misbruges til andre former for angreb – herunder distribuerede overbelastningsangreb (DDoS), hvor mange enheder bruges til at overbelaste en given tjeneste eller hjemmeside.

DDoS-angreb og cyberaktivisme mod offentlige institutioner

TDC Erhverv Security Operations Center har gennem 2025 observeret gentagne DDoS-angreb mod danske domæner – særligt rettet mod samfundsvigtige funktioner som offentlig transport, Skat og offentlige styrelser. Et DDoS-angreb (Distributed Denial of Service) er et angreb, hvor store mængder trafik sendes mod en digital tjeneste eller hjemmeside med det formål at overbelaste den og gøre den utilgængelig for brugere.

Frem til november 2025 var det primært et begrænset antal domæner – omkring 30 – der gentagne gange blev ramt. I forbindelse med kommunal- og regionsvalget i november steg antallet markant, og op mod 100 domæner blev angrebet i løbet af få dage. Timingen og intensiteten peger på koordinerede og politisk motiverede angreb snarere end tilfældig cyberkriminalitet.

Selvom de mange DDoS-angreb ikke udelukkende er rettet mod kommuner, understreger de, hvordan offentlige institutioner i stigende grad bliver mål for både cyberkriminalitet og cyberaktivisme med det formål at skabe forstyrrelser, usikkerhed og pres på samfundskritiske funktioner.

En kompleks angrebsflade kræver øget opmærksomhed

Kommuner spiller en central rolle i driften af velfærdssamfundet og håndterer store mængder data og digitale services på tværs af borgere, institutioner og samarbejdspartnere. Det gør dem til attraktive mål – ikke kun for økonomisk motiverede angreb, men også for aktører med politiske eller strategiske hensigter.

Blokeringer af ondsindede domæner er fortsat stigende

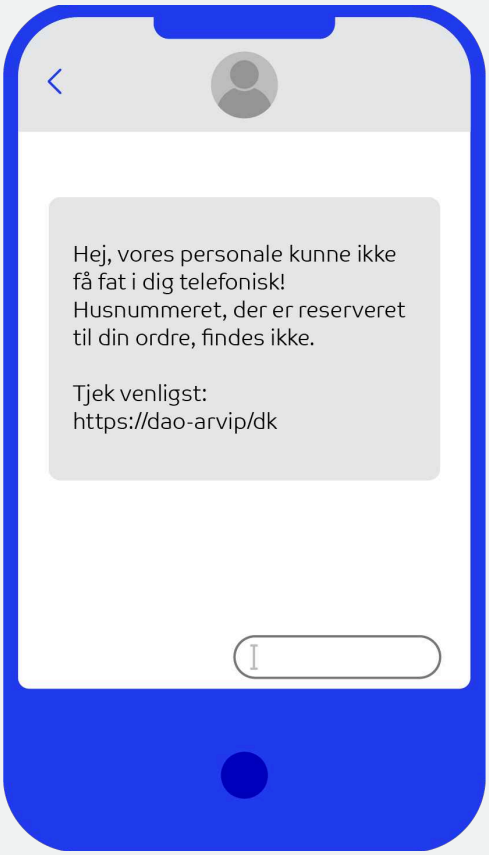
I Q1 2026 blokeredes i alt 166.479.641 forsøg på at tilgå ondsindede domæner via kablede og mobile forbindelser for privat-og erhvervskunder, og langt størstedelen af blokeringerne foregik på mobile forbindelser.

Det viser, at ondsindede aktører er interesserede i at udnytte vores vaner, vores tillid og vores nysgerrighed – uanset om vi er på arbejde eller derhjemme. Og med god grund. Medarbejdere er nemlig også privatpersoner, og deres adfærdsmønstre på private enheder kan nemt smitte af på enheder udstedt af arbejdsgiveren. Det kan fx være privat surfing på arbejdstelefonen – fordi det lige er den, der ligger tættest – eller brug af privat mail og andre online tjenester på arbejdscomputeren, som kan føre til klik på skadelige phishing-links.

Phishingkampagner forklædt som leveringstjenester rammer europæiske brugere

Et godt eksempel på udnyttelsen af vores tillid og vaner er omfattende phishingkampagner observeret i Q1 på tværs af Europa, hvor ondsindede aktører udgiver sig for at være kendte pakkeleveringstjenester som DAO, DHL og DPD. Kampagnerne distribueres typisk via smishing-beskeder sendt gennem sms, iMessage eller RCS og forsøger at lokke brugere til falske leveringssider med henblik på at stjæle betalingsoplysninger, logininformation og multifaktorgodkendelser.

Kampagnerne viser, hvordan cyberangreb i stigende grad tager udgangspunkt i velkendte hverdagssituationer og mobile brugeradfærdsmønstre – særligt i en tid, hvor arbejde og privatliv flyder mere sammen på tværs af enheder og tjenester.



Derudover kan brugen af private mobiler eller computere i arbejdssammenhæng – ofte omtalt som Bring Your Own Device (BYOD) – betyde, at grænsen mellem private og arbejdsrelaterede enheder i nogle virksomheder bliver mere flydende.

Nogle virksomheder vælger ikke at udlevere arbejdsgiverbetalte telefoner til alle medarbejdere, mens andre accepterer, at medarbejdere anvender egne enheder til arbejdsformål. Dermed kan kompromitterede apps, phishingforsøg eller ondsindede links på private enheder også udgøre en potentiel risiko for arbejdsrelaterede data systemer.

og systemer, når enhederne kobles på arbejdspladsens netværk eller bruges til at tilgå virksomhedens

Det understreger vigtigheden af ansvarlig digital adfærd, som vi tager med os på arbejde – især når grænserne mellem arbejde og fritid fortsat er flydende. De samme phishingkampagner, falske links og inficerede domæner, der rammer privatlivet, udgør også en reel risiko for virksomheder.

Få hjælp til at beskytte jer mod phishing med TDC Erhverv Internetfilter

TDC Erhverv Internetfilter er en sikkerhedsløsning bygget på DNS-filterteknologi, der forhindrer brugere i at besøge ondsindede domæner på deres computere, tablets og mobiler. Viser det sig, at domænet er klassificeret som ondsindet eller kompromitteret, bliver adgangen automatisk blokeret, inden forbindelsen overhovedet bliver oprettet, og brugeren får en advarsel på skærmen.

Sådan beskytter TDC Erhverv Internetfilter jeres medarbejdere, så de kan arbejde trygt på computer og mobiler, på arbejdet, derhjemme og på farten.

Læs mere om TDC Erhverv Internetfilter

RisePro – malwaren designet til at **stjæle jeres data**

RisePro er i Q1 2026 blandt de mest observerede malwarefamilier hos TDC Erhverv Cyber Threat Intelligence. Det viser, at informationsstjælende malware, også kaldet infostealers, fylder betydeligt i trusselsbilledet mod virksomheder i Danmark. Og hvor ransomware ofte får størst opmærksomhed, ser vi en stigende mængde malware, der arbejder langt mere diskret – og kan forsage betydelig skade.

Formålet med RisePro er ikke nødvendigvis at skabe synlig skade med det samme. Infostealeren er designet til hurtigt at udtrække følsomme data som loginoplysninger, browserdata, betalingsoplysninger, cookies og sessionsinformationer. Moderne virksomheder er dybt afhængige af digitale platforme og cloudtjenester til alt fra samarbejde og økonomi til dataopbevaring og administration. Det betyder, at fx kompromitterede loginoplysninger kan være ekstremt værdifulde, og give aktørerne adgang til et væld af kritisk data.

Sådan spredes RisePro

RisePro spredes typisk gennem phishingkampagner, kompromitterede hjemmesider eller ondsindede downloads.

Det kan fx være:

- Falske softwareopdateringer
- Piratkopierede programmer eller modificerede versioner af disse
- Dokumenter eller filer sendt via phishing-mails
- Kompromitterede hjemmesider med skjult malware
- Falske browserudvidelser eller værktøjer

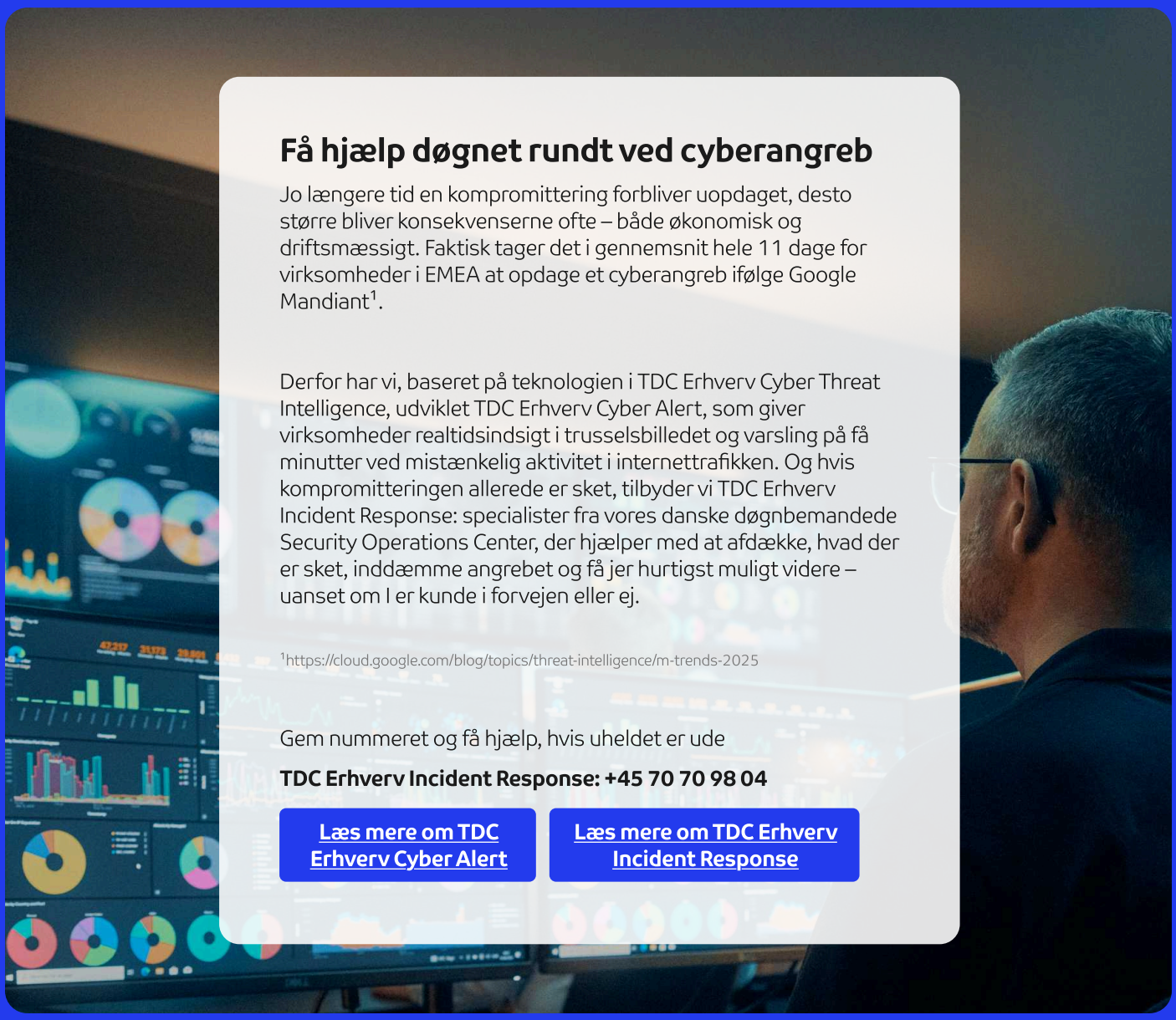
Samtidig distribueres RisePro også gennem såkaldt Malware-as-a-Service. Det betyder, at værktøjet ikke nødvendigvis bruges af én bestemt gruppe, men kan lejes eller købes af forskellige ondsindede aktører. Dermed bliver avancerede malwareværktøjer tilgængelige for langt flere, også aktører med begrænset teknisk viden. Et særligt kendetegn ved RisePro er samtidig, at malwaren løbende videreudvikles for at undgå detektion og udnytte nye indgange til systemer og brugere.

Den stille begyndelse på et større angreb

Infostealers som RisePro er særligt problematiske, fordi kompromitteringen ofte sker uden tydelige tegn. Der er ingen nedlåste systemer. Ingen krav om løsesum. Ingen tydelig nedbrudssituation. I stedet kan data indsamles stille og roligt i baggrunden, mens brugeren fortsætter sit arbejde som normalt.

De stjålne oplysninger sendes typisk videre til aktørernes infrastruktur, hvor de kan anvendes som første skridt i en større kompromittering. I nogle tilfælde sælges de stjålne oplysninger videre til andre kriminelle grupper, som efterfølgende bruger adgangen til mere målrettede angreb. Dermed bliver infostealers en del af et større kriminelt økosystem, hvor forskellige aktører specialiserer sig i hver deres del af angrebskæden.

For virksomheder i Danmark understreger udviklingen behovet for både tekniske sikkerhedslag og fokus på sikker digital adfærd. For selv mindre kompromitteringer kan udvikle sig til langt større hændelser, hvis de ikke opdages i tide.



Få hjælp døgnet rundt ved cyberangreb

Jo længere tid en kompromittering forbliver uopdaget, desto større bliver konsekvenserne ofte – både økonomisk og driftsmæssigt. Faktisk tager det i gennemsnit hele 11 dage for virksomheder i EMEA at opdage et cyberangreb ifølge Google Mandiant[1].

Derfor har vi, baseret på teknologien i TDC Erhverv Cyber Threat Intelligence, udviklet TDC Erhverv Cyber Alert, som giver virksomheder realtidsindsigt i trusselsbilledet og varsling på få minutter ved mistænkelig aktivitet i internettrafikken. Og hvis kompromitteringen allerede er sket, tilbyder vi TDC Erhverv Incident Response: specialister fra vores danske døgnbemandede Security Operations Center, der hjælper med at afdække, hvad der er sket, inddæmme angrebet og få jer hurtigst muligt videre – uanset om I er kunde i forvejen eller ej.

[1]https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025

Gem nummeret og få hjælp, hvis uheldet er ude

TDC Erhverv Incident Response: +45 70 70 98 04

Læs mere om TDC Erhverv Cyber Alert

Læs mere om TDC Erhverv Incident Response