

TDC Erhverv Sikkerhedsrapport Q3 2026

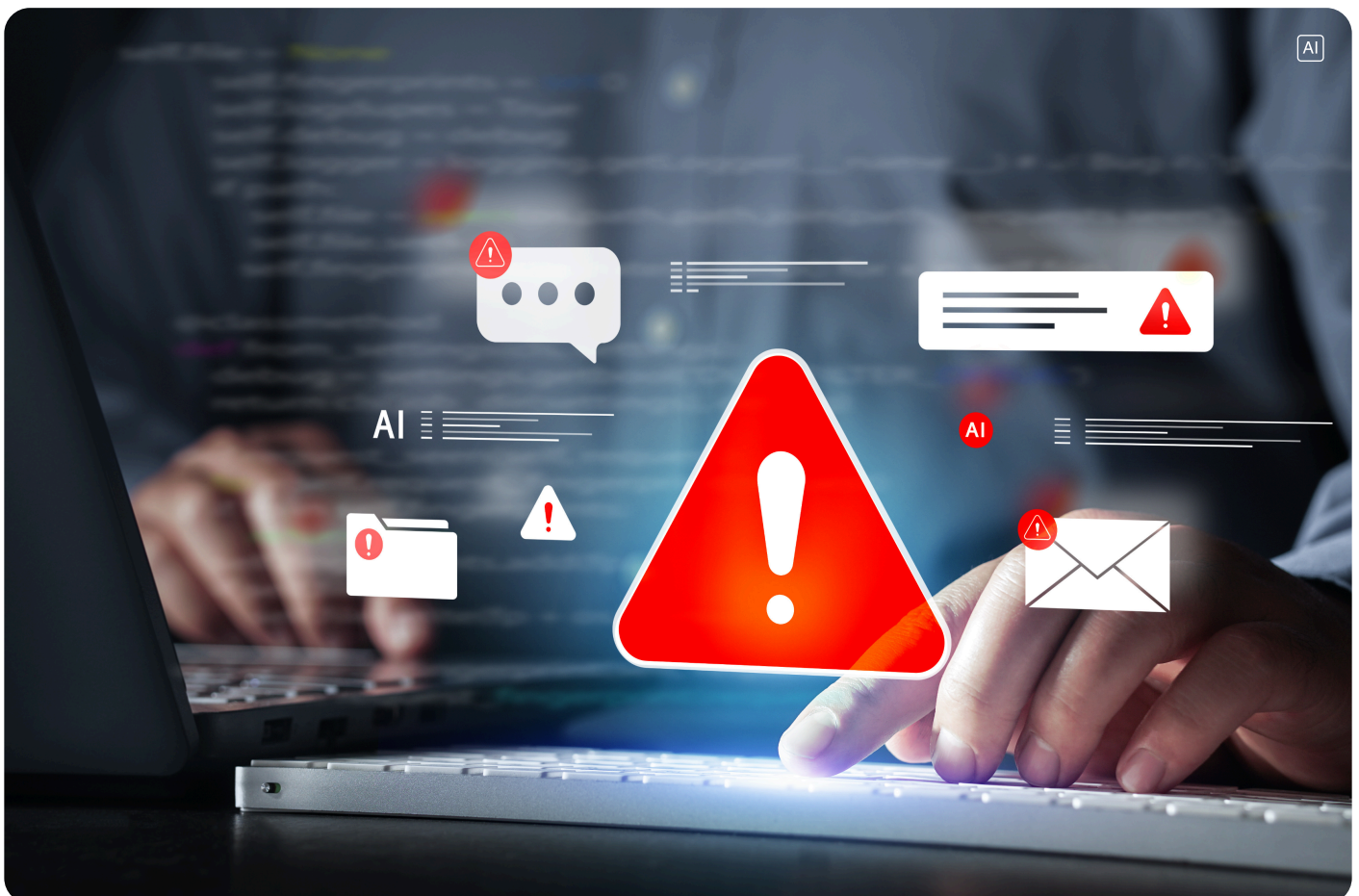
Q3, kort fortalt

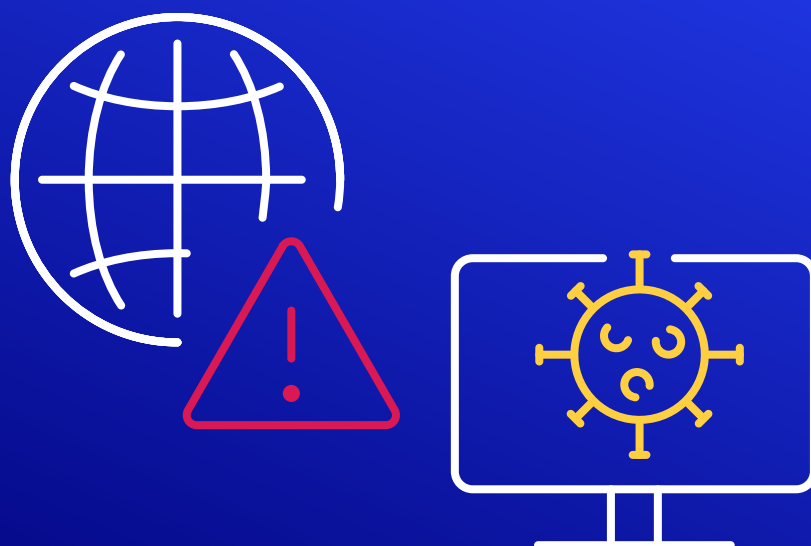
I tredje kvartal 2026 observerede TDC Erhverv Cyber Threat Intelligence aktiviteter hos 2.388 danske virksomheder og organisationer, hvor trafikken indikerede malware-relaterede hændelser. Observationerne viser et trusselsbillede, hvor cyberkriminelle både udnytter interneteksponerede systemer og almindelige digitale vaner som veje til kompromittering. I september hævede Styrelsen for Samfundssikkerhed desuden trusselsniveauet for destruktive cyberangreb mod Danmark fra middel til høj på baggrund af et skærpet trusselsbillede vurderet af FE.

Tre observationer skiller sig særligt ud:

- Mirai-relateret aktivitet udgjorde 53,93 % af de observerede hændelser i kvartalet og er fortsat den mest observerede malwarefamilie i Q3, ligesom i Q2.
- Virksomheder og organisationer med mere end 1.000 ansatte stod for første gang i år for mere end en tredjedel af de observerede hændelser.
- TDC Erhverv observerede aktivitet relateret til SectopRAT, som indgår i internationale kampagner, hvor søgemaskiner, annoncer og falske softwaredownloads anvendes til at distribuere malware.

På tværs af kvartalets observationer ser vi, hvordan cyberkriminelle udnytter både teknologi og menneskelig adfærd som veje til kompromittering. Særligt observationerne omkring SectopRAT viser, hvordan populære værktøjer og AI-relaterede tjenester kan bruges som lokkemidler i angrebekampagner. Det understreger vigtigheden af både tekniske sikkerhedskontroller og opmærksomme medarbejdere.





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.

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 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. Resultatet er dansk trusselsindsigt, som giver os og vores kunder et unikt forspring i arbejdet mod cyberangreb.

Note: 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.

Q3 2026 i tal

2.388

Hændelser blandt virksomheder og organisationer i Danmark, der indikerer kompromittering med malware i Q3 2026.

I Q3 2026 observerede TDC Erhverv Cyber Threat Intelligence aktiviteter hos **2.388** virksomheder og organisationer, hvor trafikken indikerede malware-relaterede hændelser.

Kvartalet var samtidig præget af en væsentlig udvikling i det overordnede trusselsbillede, da Styrelsen for Samfundssikkerhed hævede trusselsniveauet for destruktive cyberangreb mod Danmark fra middel til høj efter FEs vurdering af øget russisk hybrid aktivitet mod NATO og Vesten.

Den hævede trusselvurdering er ikke ensbetydende med, at et konkret angreb er nært forestående, men den understreger betydningen af robuste sikkerheds- og beredskabsforanstaltninger i danske virksomheder og organisationer. Du kan læse TDC Erhvervs samlede vurdering af det hævede trusselsniveau [her](#).

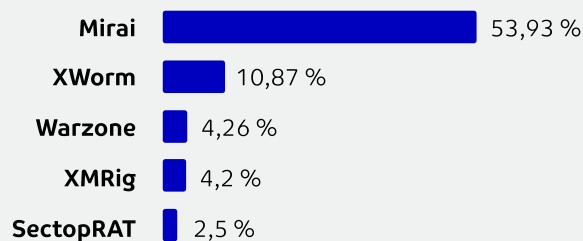
Mirai dominerer fortsat datagrundlaget og stod alene for **53,93 %** af de observerede hændelser, mens SectopRAT for første gang optræder blandt de fem mest observerede malwarefamilier.

SectopRAT er særligt interessant i denne omgang, fordi observationerne viser, hvordan cyberkriminelle kan udnytte almindelige digitale vaner som søgninger, softwaredownloads og interessen for AI-relaterede værktøjer som en del af kompromitteringsforsøg.

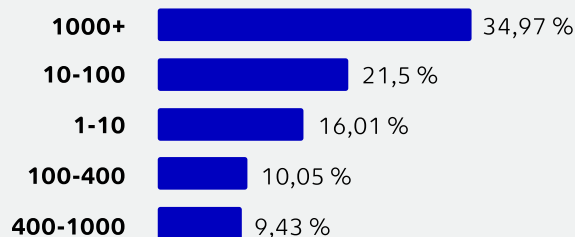
Organisationer med mere end 1.000 ansatte udgør den største andel af de observerede hændelser i kvartalet. IT-branchen ligger igen øverst blandt de observerede hændelser og stod for **16,31 %** af de registrerede observationer. I lighed med tidligere kvartaler, ligger branchen fortsat i top.



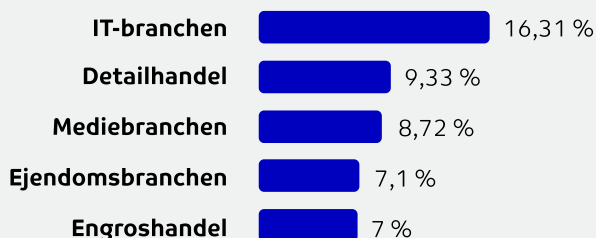
Mest observerede malwarefamilier



Virksomhedsstørrelser (Ansatte)



Brancher



Når cyberkriminelle udnytter søgemaskiner og vaner

SectopRAT var blandt de fem mest observerede malwarefamilier i Q3 2026. Vores observationer peger på kompromitteringsforsøg, hvor cyberkriminelle anvender manipulerede søgeresultater, annoncer, falske softwaredownloads og AI-hypen til at kompromittere virksomheder og organisationer. Dette adskiller sig fra de mere automatiserede hændelser relateret til f.eks. Mirai, som vi beskrev i vores Q2 rapport.

De fleste virksomheder betragter søgemaskiner som et naturligt redskab til informationssøgning, softwaredownloads og adgang til digitale tjenester. Cyberkriminelle forsøger imidlertid også at udnytte den tillid og de vaner, der er forbundet med søgninger, softwaredownloads og brugen af velkendte værktøjer.

Det kan eksempelvis ske gennem manipulerede søgeresultater, betalte annoncer eller hjemmesider, der udgiver sig for at være officielle softwareportaler. På denne måde ender brugeren selv med at opsoge det indhold, som angribereren ønsker, at offeret skal finde.

For den enkelte medarbejder kan oplevelsen fremstå legitim. Søgeresultatet ser troværdigt ud, hjemmesiden ligner den rigtige, og installationsfilen fungerer ofte som forventet. Det er først efter installationen, at malware aktiveres, og kompromitteringen finder sted.

Fra søgning til kompromittering

Et typisk angreb følger ofte et relativt simpelt forløb. Medarbejderen søger efter et program eller et værktøj, som skal bruges i det daglige arbejde. Blandt søgeresultaterne vises enten en annonce eller et manipuleret søgeresultat, som leder videre til en falsk hjemmeside. Herfra downloades en installationsfil, der ser legitim ud, men som i virkeligheden indeholder malware. Når programmet installeres, får angribereren adgang til enheden eller mulighed for at stjæle information fra den kompromitterede enhed.

Det gør denne type angreb særligt effektiv, fordi brugeren selv gennemfører de handlinger, der fører til kompromitteringen.

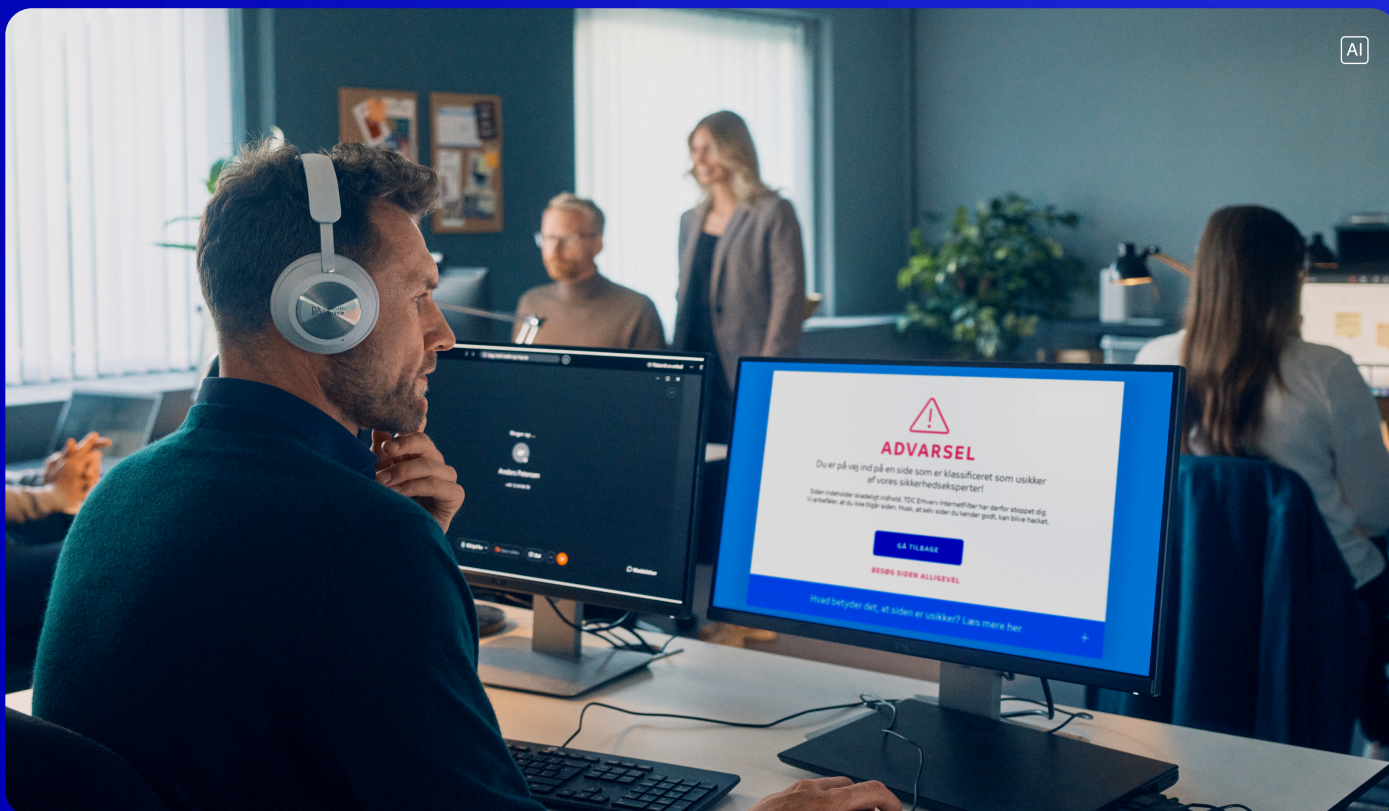
Hvorfor AI-værktøjer er attraktive lokkemidler

Cyberkriminelle tilpasser ofte deres kampagner til de værktøjer og teknologier, som virksomheder aktuelt interesserer sig for. Observationerne i Q3 viser, at AI-relaterede værktøjer kan være attraktive lokkemidler i kompromitteringsforsøg.

Tjenester som Claude Desktop, Docker Desktop, Google Chrome og GitHub indgår i mange medarbejders daglige arbejdsprocesser og har samtidig en høj troværdighed. Når nye værktøjer hurtigt bliver populære, kan der opstå et tidsvindue, hvor organisationer endnu ikke har etableret faste procedurer for installation, distribution og kontrol. Det kan give cyberkriminelle mulighed for at udnytte interessen gennem falske downloadsider og annoncer.

Observationerne understreger, at populære digitale værktøjer ikke kun er produktivitetsteknologier. De kan også blive en del af cyberkriminelles sociale manipulationsstrategier.





SEO poisoning førte til kompromittering

SectopRAT er en malwarefamilie, der kombinerer egenskaber fra en Remote Access Trojan (RAT) og en informationsstjæler. Når malware installeres på en enhed, kan den både give angriberen fjernadgang til enheden og indsamle følsomme oplysninger fra den kompromitterede bruger.

TDC Erhverv observerede SectopRAT-aktivitet fra midten af juli 2026, og observationerne stemmer bl.a. tidsmæssigt overens med internationale kampagner*, hvor der blev anvendt både SEO poisoning og malvertising til distribution. SEO poisoning er en teknik, hvor angribere manipulerer søgeresultater for at få skadelige hjemmesider til at fremstå legitime. Malvertising dækker over misbrug af onlineannoncer til at lokke brugere videre til skadeligt indhold.

Teknikkerne er interessante, fordi de illustrerer, hvordan angriberne udnytter vores vaner og beslutninger. I stedet for alene at forsøge at bryde tekniske sikkerhedsforanstaltninger ned forsøger de også at påvirke brugernes adfærd og valg.

Hvem bliver ramt?

Observationerne i Q3 omfatter blandt andet organisationer inden for telekommunikation, sundhedsvæsen, uddannelse, IT-sektoren, kommuner og sociale tilbud.

Aktiviteten er dermed ikke begrænset til én bestemt sektor. Tværtimod peger observationerne på, at kampagnerne rammer bredt på tværs af organisationstyper, hvor digitale værktøjer spiller en central rolle i hverdagen.

Samtidig er der ikke identificeret virksomheder med mellem 1 og 10 ansatte blandt de observerede tilfælde. Observationerne peger derfor forsigtigt på, at kompromitteringsforsøgene i højere grad har ramt organisationer, hvor medarbejdere anvender specialiserede softwareværktøjer og digitale platforme som en central del af arbejdet.

Hvad betyder det for virksomheder?

Observationerne viser, at kompromitteringsforsøg ikke kun handler om tekniske sårbarheder, men også om brugernes adfærd og organisationens processer. Virksomheder kan blandt andet reducere risikoen gennem følgende tiltag:

- Download software fra officielle kilder: Begræns installation af software til godkendte app stores, leverandørernes officielle hjemmesider eller internt godkendte distributionskanaler.
- Reducer risikoen teknisk: DNS- og internetfiltrering kan hjælpe med at blokere kendte skadelige domæner. Løsninger som TDC Erhverv Internetfilter kan være et supplement til organisationens øvrige sikkerhedskontroller.
- Træn medarbejdere: Medarbejdere bør kende risikoen ved SEO poisoning, malvertising og falske softwareportaler og være særligt opmærksomme.

*Blandt andet beskrevet af Huntress: Inside FakeAgent: How a Claude Desktop Malvertising Campaign Hit 29 Organizations with SectopRAT | Huntress

Fra kompromitterede enheder til proxynetværk

Proxy- og relay-infrastruktur var ikke blandt de største malwarekategorier i Q3, men observationerne er alligevel interessante. TDC Erhverv observerede aktivitet relateret til blandt andet Ngioweb, distribueret ORB-/relay-infrastruktur samt malwarefamilier som Warzone og Remcos. Fælles for observationerne er, at de illustrerer, hvordan kompromitterede systemer ikke alene kan bruges til direkte angreb, men også som infrastruktur for andre aktørers aktiviteter.

Værdien af en kompromitteret enhed ligger ikke nødvendigvis i data eller adgang til virksomheden. I nogle tilfælde er selve internetforbindelsen, IP-adressen eller muligheden for at videresende trafik det attraktive mål.

Et proxynetværk består af enheder, der fungerer som mellemed for internettrafik. Når trafikken sendes gennem en proxy, vil den typisk fremstå som om, den kommer fra proxyens IP-adresse og ikke fra den oprindelige afsender.

Proxynetværk anvendes også til legitime formål. I en cyberkriminel sammenhæng kan de imidlertid bestå af kompromitterede routere, servere eller IoT-enheder, som bruges til at videresende trafik uden ejerens viden.

Hvor kommer enhederne fra?

Enhederne kan komme fra både private hjem og virksomheder og omfatter blandt andet routere, IoT-enheder, servere og andre internetforbundne systemer. De kan blive en del af et proxynetværk gennem malware, udnyttelse af sårbarheder eller kompromitterede adgangsuplysninger.

Observationerne fra Q3 viser aktivitet relateret til proxy- og relay-infrastruktur på tværs af flere brancher. En del af infrastrukturen befinder sig i almindelige internet- og accessnetværk frem for traditionelle hostingmiljøer, hvilket er konsistent med brugen af kompromitterede enheder som proxy-noder.

Hvorfor er proxynetværk attraktive for cyberkriminelle?

Proxynetværk gør det muligt at adskille en aktørs egen infrastruktur fra den aktivitet, der udføres på internettet. Når trafikken sendes gennem kompromitterede enheder, kan den fremstå som legitim trafik fra almindelige privat- eller virksomhedsforbindelser.

Det gør det vanskeligere at identificere trafikens egentlige oprindelse og giver samtidig mulighed for løbende at skifte mellem IP-adresser. Sådanne netværk kan bruges til blandt andet scanning, angreb, omgåelse af sikkerhedskontroller eller økonomisk motiveret svindel.

Proxy- og relay-infrastruktur kan desuden både anvendes til at understøtte ondsindet aktivitet og til økonomisk motiverede formål såsom videresalg af internettrafik.

Hvad observerede vi i Q3?

I analysen af Q3-data observerede TDC Erhverv flere former for aktivitet, som kan forbindes med proxy- og relay-infrastruktur. Blandt observationerne indgår Ngioweb (også kaldet NSOCKS), distribueret ORB-/relay-infrastruktur samt malwarefamilierne Warzone og Remcos, som alle kan anvendes til at videresende trafik via kompromitterede systemer.

Observationerne understreger, at kompromitterede systemer kan være værdifulde for angribere, selv når formålet ikke er datatyveri eller afpresning af den konkrete organisation.

Hvad betyder det for virksomheder?

For virksomheder handler kompromittering ikke kun om risikoen for datatyveri eller nedbrud. En kompromitteret router, server eller anden internetforbundet enhed kan også blive udnyttet som proxy eller relay for aktiviteter rettet mod andre organisationer. Det betyder, at jeres internetforbindelse og offentlige IP-adresser i sig selv kan være en attraktiv ressource for cyberkriminelle.

Derfor bør organisationer løbende vurdere, hvilke systemer der er eksponeret mod internettet, om eksponeringen er nødvendig, og om den er tilstrækkeligt beskyttet. Samtidig kan overvågning af usædvanlig udgående trafik hjælpe med at identificere kompromitterede enheder tidligt.

Da ransomware ramte: Fra alarm til handling

TDC Erhverv tilbyder Security Operations og Incident Response-løsninger. I juni 2026 assisterede vores Incident Response-team med håndteringen af en ransomwarehændelse hos en europæisk organisation. I forbindelse med undersøgelsen blev også trusselsindsigter fra vores cyber threat intelligence arbejde anvendt til at understøtte håndteringen.

Undersøgelsen viste et angreb, der udviklede sig fra kompromittering af legitim fjernadgang til fuld kontrol over virksomhedens centrale system til styring af brugere, computere og adgangsrettigheder (Active Directory). Herefter stjal angriberen data fra organisationen (dataeksfiltration), før ransomware blev installeret og aktiveret på tværs af miljøet.

Der gik 13 dage fra det første identificerede credential-angreb til ransomware blev installeret. Størstedelen af perioden var præget af begrænset aktivitet, før aktøren på få timer eskalerede til fuld kompromittering af miljøet.

De første tegn

Hændelsen blev identificeret efter mistænkelige VPN-logins, privilegeret aktivitet med domæneadministratorrettigheder og oprettelsen af skadelige planlagte opgaver. På flere servere blev der fundet ransomwarenotes fra gruppen "The Gentlemen".

Håndteringen

TDC Erhvervs Incident Response-team arbejdede i to spor: dels med at rekonstruere angrebsskæden og identificere initial access, dels med at etablere grundlaget for en kontrolleret recovery.

Eksisterende SIEM-telemetri fra VPN-, Windows- og netværkskilder gjorde det muligt hurtigt at identificere den kompromitterede konto og kortlægge forløbet fra de første authentication events til ransomware-deployment.

Samspeilet mellem Threat Intelligence og Incident Response

Hændelsen viser værdien af samspeilet mellem Threat Intelligence og Incident Response. Trusselsindsigt hjælper med at identificere kendte teknikker og adfærdsmønstre, mens Incident Response omsætter denne viden til konkrete handlinger i det kompromitterede miljø. I den konkrete sag bidrog eksisterende telemetri og analyser til hurtigere at kortlægge angrebet og understøtte en kontrolleret genopretning.

Tre læringer

1

Tidlig opdagelse betyder alt. Aktøren havde adgang til miljøet i næsten to uger før der blev lagt ransomware på systemerne. Observationen understreger værdien af tidlig detektion og overvågning af mistænkelig autentificeringsaktivitet.

2

Angreb udvikler sig hurtigt. Efter kompromittering af domænet gik der blot få timer, før angriberen var i stand til at gennemføre en omfattende ransomware-deployment.

3

Forberedelse reducerer konsekvenserne. Hændelsen viste værdien af bred sikkerhedstelemetri og veldefinerede response-processer. Adgangen til historiske data gjorde det muligt at rekonstruere angrebet og understøtte en kontrolleret genopretning.

[Læs hele casen her](#)

Hvad kan virksomheder tage med fra Q3?



Kend jeres eksponering

Observationerne fra Q3 understreger betydningen af at have overblik over både interneteksponerede systemer, fjernadgange og enheder, der kommunikerer med internettet. Kompromittering handler ikke kun om risikoen for datatyveri eller driftsforstyrrelser. En kompromitteret enhed kan også blive udnyttet som en del af den infrastruktur, der bruges til at understøtte andre cyberkriminelle aktiviteter. Derfor er det afgørende løbende at identificere, hvilke systemer der er eksponeret mod internettet, hvorfor de er eksponeret, og om eksponeringen fortsat er nødvendig.



Vær kritisk over for søgeresultater og softwaredownloads

Cyberkriminelle forsøger ikke kun at udnytte tekniske sårbarheder. De udnytter også vaner og tillid. Observationerne omkring SectopRAT viser, hvordan annoncer, manipulerede søgeresultater og falske softwareportaler kan bruges som en del af angrebsvejen. Medarbejdere bør derfor være opmærksomme på, hvor software hentes fra, og organisationer bør så vidt muligt anvende officielle distributionskanaler og etablerede procedurer for installation af nye værktøjer. Teknologier som TDC Erhverv Internetfilter kan samtidig være med til at reducere risikoen for, at medarbejdere eksponeres for kendte skadelige domæner og downloadsites.



Priorité overvågning og tidlig detektion

I ransomware-casen gik der 13 dage fra den første identificerede kompromittering til ransomware blev implementeret. Størstedelen af perioden var præget af begrænset aktivitet, før angrebet eskalerede hurtigt. Det understreger værdien af løbende overvågning, logning og sikkerhedsteleometri, der kan identificere mistænkelig aktivitet. Løsninger, der overvåger og varsler om potentiel kompromittering, kan bidrage til et bedre overblik over organisationens eksponering. Eksempelvis kan TDC Erhverv Cyber Alert hjælpe med at identificere indikatorer på kompromittering og gøre organisationer opmærksomme på potentielle trusler på få minutter, før de udvikler sig.



Hav en plan, før noget sker

Når et cyberangreb udvikler sig, er tiden ofte en kritisk faktor. Organisationer, der på forhånd har afklaret roller, ansvar, kommunikationsveje og beslutningsprocesser, har typisk bedre forudsætninger for at håndtere hændelsen effektivt. Incident Response starter derfor ikke, når angrebet opdages. Den starter med forberedelsen, øvelserne og de processer, der er etableret på forhånd.

Få hurtig hjælp ved cyberangreb

Når et cyberangreb rammer, er hurtig handling afgørende for at begrænse konsekvenserne. Med **TDC Erhverv Incident Response** har I adgang til specialister, der kan hjælpe ved mistanke om eller aktive cyberhændelser.

Vores Security Operations Center står klar døgnet rundt til at analysere hændelsen, begrænse skaden og hjælpe jer sikkert videre.

Ring (+45) 70 70 94 08 ved mistanke om et cyberangreb.

Få hurtig hjælp ved cyberangreb

Styrk jeres cyberberedskab gennem øvelse

Cybersikkerhed handler ikke kun om teknologi. Det handler også om at træne samarbejde, beslutningstagning og beredskab, før en hændelse opstår.

Derfor gennemføres der i oktober cyberøvelser på tværs af Danmark, Færøerne og Grønland som en del af initiativet Hele Danmark Øver. Øvelserne giver virksomheder og organisationer mulighed for at teste deres beredskab og styrke evnen til at håndtere cyberhændelser i praksis.

Styrk jeres cyberberedskab gennem øvelse