Hvordan beskytter vi nettet og tjenestene våre?

Mats S. Olsen

NTE Telekom AS

Kritisk infrastruktur

Hva er det?

Systemer og tjenester samfunnet er avhengig av – som strøm, vann, transport og telekommunikasjon.

Hvorfor er det viktig?

Svikt eller angrep kan få alvorlige konsekvenser for sikkerhet, helse og økonomi.

Nye utfordringer

Digitalisering gir effektivitet, men øker risikoen for cyberangrep og tekniske feil.

DDoS – Distribuert tjenestenekt

Hva er DDoS?

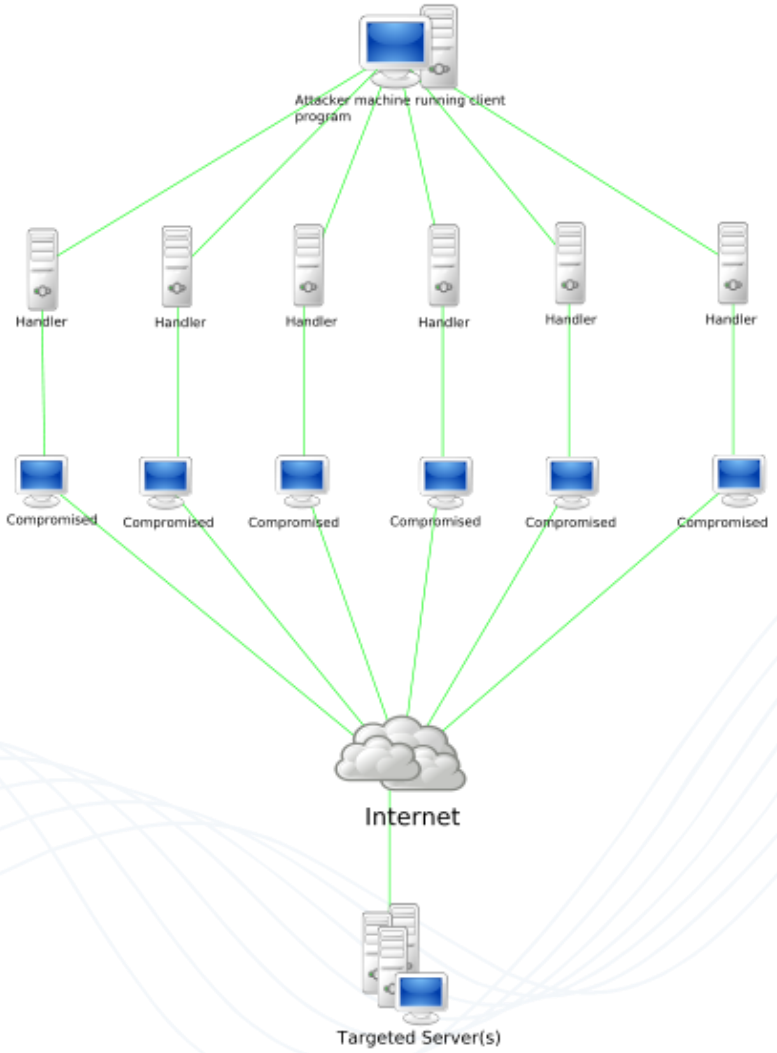
Et angrep som hindrer tilgang til informasjon eller tjenester ved å overbelaste systemet med trafikk.

Hvordan fungerer det?

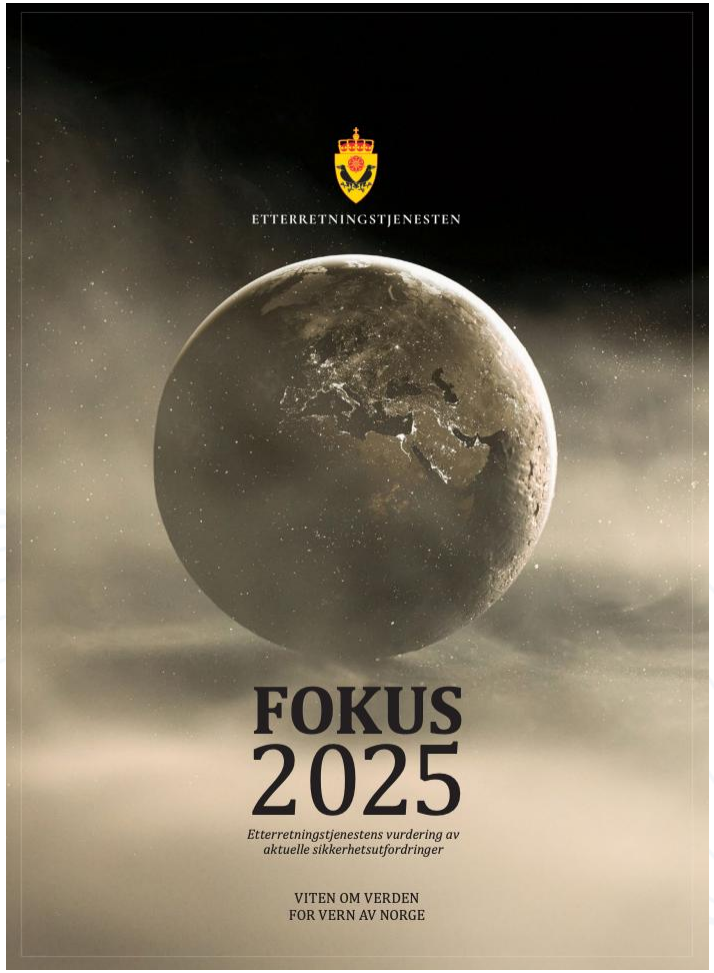
Angrepet utføres ofte via et botnet – en samling infiserte datamaskiner som styres fra én sentral server. Eierne vet som regel ikke at de er berørt.

Hvorfor er det farlig?

Botnet kan generere enorme mengder trafikk (gigabit/terabit per sekund) og lamme viktige digitale tjenester.



Trusselvurderinger 2025



Cybertrusselen

Økt risiko for sabotasje

Trusselvurderinger viser at sabotasjeforsøk i Norge er sannsynlig. NSM anbefaler forebyggende tiltak nå.

Kritiske innsatsfaktorer

Strøm, vann, transport, internett og PNT (posisjon, navigasjon og tid) må sikres mot bortfall.

Rask respons er avgjørende

Evne til å gjenopprette tjenester raskt er viktig for å opprettholde samfunnssikkerhet.

Historiens største IT-kollaps

Utilsiktede hendelser kan gjøre like stor skade som et alvorlig dataangrep. Flyplasser, banker, hoteller, børser, sykehus, apotek, bensinstasjoner og flere ble sommeren 2024 rammet av det som omtales som «historiens største IT-kollaps». En feil i en programvareoppdatering i et antivirus-program fra datasikkerhetsselskapet Crowdstrike førte til at rundt 8,5 millioner datamaskiner krasjet globalt. Relativt få virksomheter i Norge ble rammet fordi programvaren er mindre utbredt her enn i mange andre land. Statistikk fra EU viser at skade som følge av tilfeldige uønskede hendelser er større enn skade som følger av uønskede hendelser forårsaket av tilsiktede handlinger.

Nye DDoS

Bekreft

- Det er klart - vi skal til Norge, sk

tirsdag ettermiddag.

efter: Utsatt for

tt i 18 land: Sjekk om du

Nett-stresstest applikasjonen Low Orbit Ion Cannon brukes i angrepene.

Så enkelt er det

***Oppdatert:* Slik klarer Anonymous å stenge**

Torsdag 9. desember 2010 kl. 10:46
Av Trond Bie

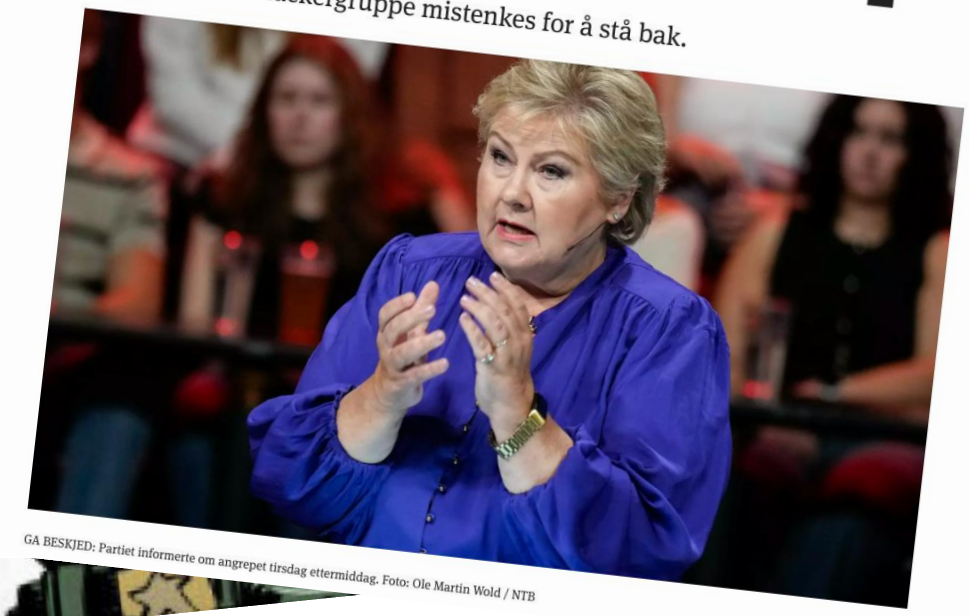
DDoS-angrepene mot MasterCard, Visa og PayPal ut
applikasjonen LOIC (Low Orbit Ion Cannon). Angrep
men styres aktivt ved hjelp av IRC og Twitter.

Slik gjør de det
Ifølge Wikipedia er LOIC en C#-applikasjon utviklet
«praetox» og andre fra 4chan. Applikasjonen DDoS
oversvømme serveren med TCP, UDP eller HTTP-pa

Programmet ble først brukt av anonymous for å a

Høyre utsatt for cyberangrep

En pro-russisk hackergruppe mistenkes for å stå bak.



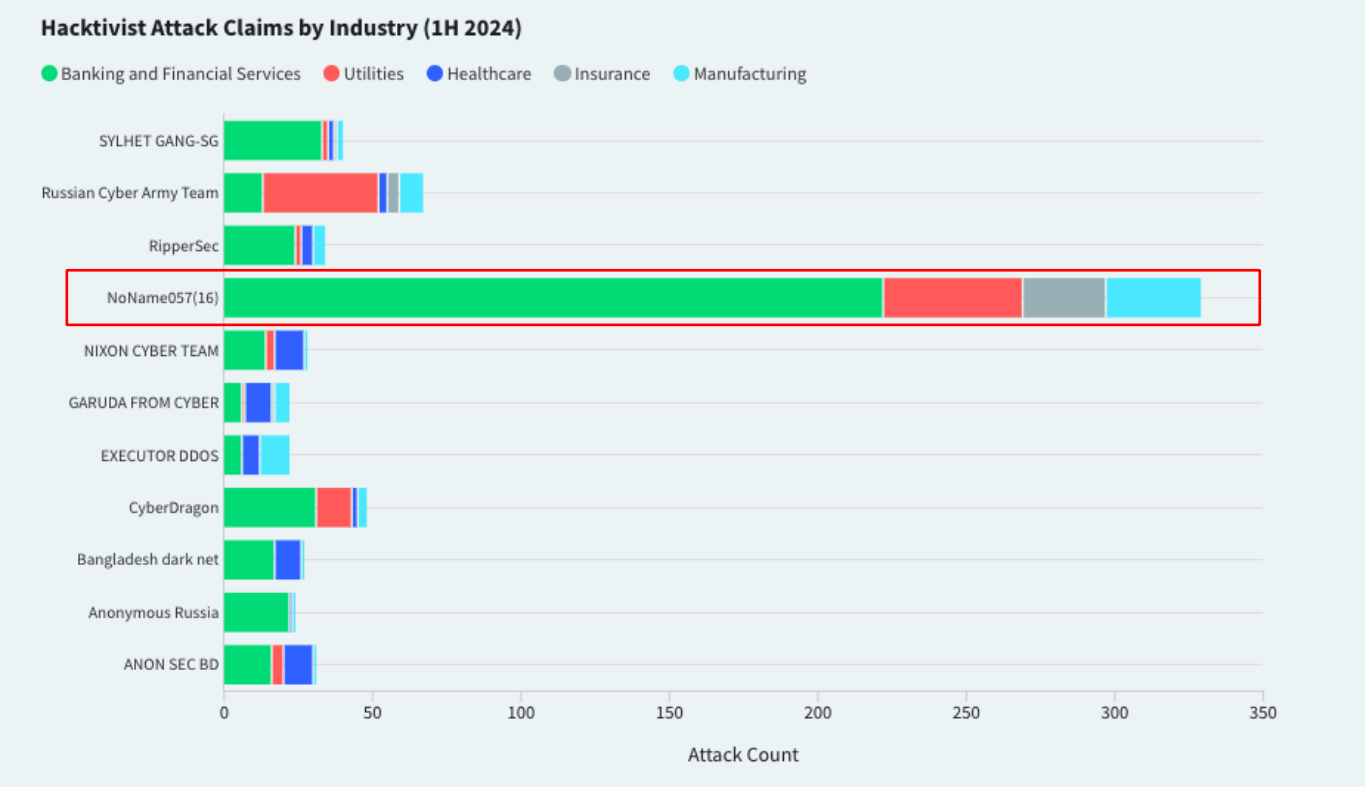
GA BESKJED: Partiet informerte om angrepet tirsdag ettermiddag. Foto: Ole Martin Wold / NTB

Vis mer

10-tida tirsdag. 📸: Ole Petter Baugerød Stokke

Escalating Threats to Critical Infrastructure

Service availability in critical industries such as banking, financial services, government, and public utilities is of paramount importance. Disruptions in these sectors can have wide-reaching consequences for both civilian populations and national security. Given our assessment that all network types can come under significant traffic load from DDoS attacks, it is crucial to understand the specific trends affecting these industries.



https://www.netscout.com/threatreport/ddos-targets/

Hackergrupper

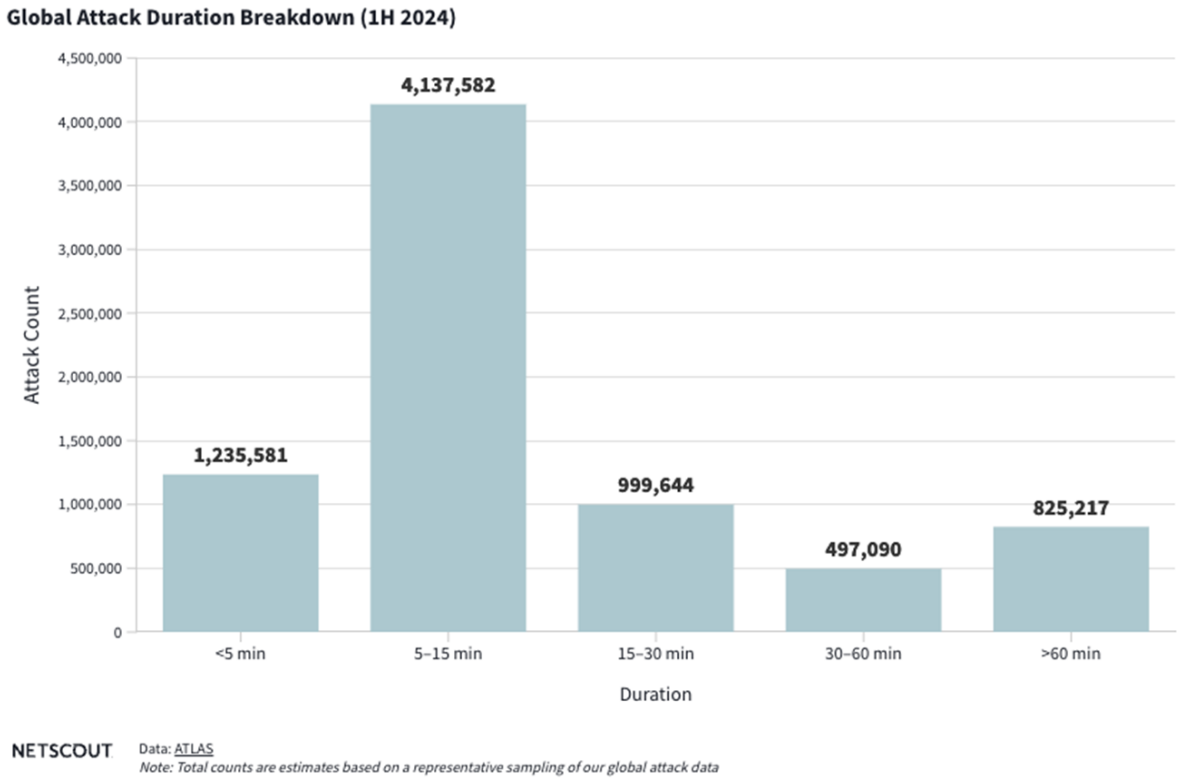
NoName057 (16)

Pro-russisk hackergruppe kjent for **DDoS-angrep** mot nettsider til myndigheter, medier og private selskaper i **Ukraina**, **USA** og **Europa**.

Salt Typhoon

Avansert vedvarende trusselaktør (APT), antatt styrt av **Kinas Ministerium for Statssikkerhet**. Aktiv siden minst 2020, kjent for omfattende spionasjekampanjer mot **telekomnettverk** i **USA** og **andre land**.

DDoS Attack Trends



DURATION BY PERCENTAGE	
<5 min	16%
5–15 min	54%
15–30 min	13%
30–60 min	6%
>60 min	11%

Risikobildet

Offentlige vurderinger

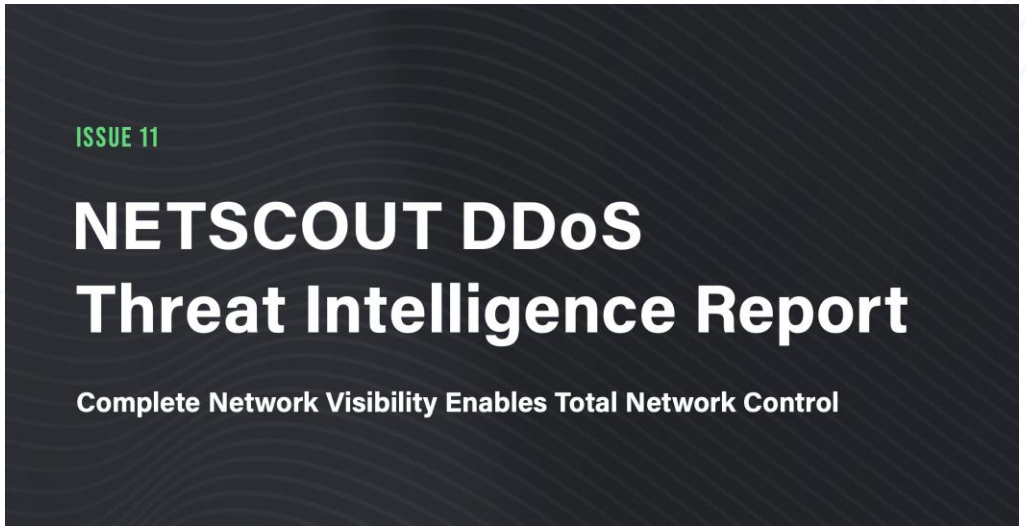
PST, NSM og Etterretningstjenesten legger frem sin risikovurdering i februar hvert år.

Egenvurderinger fra aktører

Store aktører som DNB publiserer egne sikkerhetsvurderinger.

Internett-trusler

Netscout legger frem sin vurdering to ganger i året.



TAKK!

Mats Olsen

leder nettutvikling

957 21 231 | mso@nte.no