Pressmeddelande
20 februari 2026

Ransomware-attacker fortsätter öka – men lägre krav från utpressarna

För första gången på fyra år minskar de begärda lösensummorna vid ransomware, samtidigt som attackerna är fler än någonsin

Den nya årsrapporten från cybersäkerhetsföretaget Arctic Wolf visar på tydliga förändringar i hur cyberbrottsligheten arbetar. Enligt 2026 Threat & Predictions Report har den begärda lösensumman vid ransomware-attacker minskat med nästan hälften, till i genomsnitt motsvarande 3,7 miljoner kronor (414 000 dollar). Ransomware är dock fortfarande det största cyberhotet mot företag och offentliga verksamheter – antalet attacker fortsätter att öka.

– Vi ser de lägre kraven på lösensummor som en medveten strategi för att öka sannolikheten för att få betalt. Samtidigt finns det flera kända exempel som visar att utpressarna fortfarande lyckas med att komma över stora belopp, säger Christopher Fielder, fälttekniker på Arctic Wolf.

En annan trend som framgår av den nya rapporten är att angriparna strävar efter att göra det så enkelt som möjligt för sig själva, vilket påverkar deras val av metoder. Det är exempelvis lättare att logga in än att hacka sig in och att stjäla data direkt än att först kryptera det, liksom att utnyttja välkända, betrodda verktyg hellre än komplexa sårbarheter.

Ransomware fortsätter att dominera hotbilden

2025 svarade ransomware för 44 procent av alla de incidenter som hanterades av Arctic Wolfs specialistteam. Andra vanliga typer av attacker var skadlig e-post (26 procent) och dataförluster som inte berodde på ransomware (22 procent).

I de ransomware-fall som hanterades av Arctic Wolf under 2025 uppgick kraven på lösensumma till totalt 2,8 miljarder kronor (302 miljoner dollar). Men sammanlagt betalades bara knappt 150 mkr ut i dessa fall (16,5 miljoner dollar). 77 procent av de drabbade organisationerna valde att inte betala och i de fall där förhandlingar fördes sänktes kraven med i genomsnitt 67 procent. Bara cirka fem procent av de ursprungligen begärda beloppen hamnade till sist hos brottslingarna.

Krav på lösensumma sätts inte slumpmässigt. Cyberbrottslingarna analyserar noggrant sina offer innan de ställer sina krav: bransch, omsättning, effekterna av driftstopp och till och med om företaget har en cyberförsäkring.

Goda säkerhetsrutiner stärker försvaret

Ett effektivt försvar mot ransomware börjar med grundläggande hygienfaktorer som flerfaktorsautentisering, robusta och testade backuprutiner, snabb patchning av sårbarheter och begränsning av användarrättigheter. Dessutom krävs tydliga och välövade beredskapsplaner för att kunna reagera snabbt och kontrollerat vid en attack.

– Tidig upptäckt är den absolut viktigaste faktorn för att begränsa konsekvenserna av en attack. Om vi som försvarare kan identifiera skadlig aktivitet innan angriparen kan aktivera ransomware eller komma över behörigheter, gör det en dramatisk skillnad i form av kostnader, avbrott och störningar i verksamheten. Med god beredskap kan vi agera mer beslutsamt, säger Kerri Shafer Page, chef för incidentrespons på Arctic Wolf.

Några slutsatser från 2026 Arctic Wolf Threat & Predictions Report:

- Ransomware, komprometterad e-post och dataincidenter svarade för 92% av fallen där Arctic Wolfs incidenthantering. Dataincidenterna ökade från 2% till 22%, vilket visar att angriparna i allt högre grad fokuserar på datastöld och utpressning.
- 5% av insatserna gjordes i förberedande faser av ransomware-attacker. Detta visar att tidig upptäckt och snabba motåtgärder kan stoppa attacker och förhindra kryptering.
- I 77% av fallen med ransomware betalades ingen lösensumma. När de gjorde det minskade professionella förhandlingar kraven med i genomsnitt 67%.
- Missbruk av verktyg för fjärråtkomst ökar kraftigt. Detta har visat sig vara en enklare metod för angripare än att utnyttja sårbarheter genom typiska hackarmetoder.
- Nätfiske stod för 85% av e-postattacker. Ökningen drivs på av möjligheterna att utnyttja AI för att skapa mer övertygande bluffmeddelanden och genomföra storskaliga attacker.
- Alla de vanligaste sårbarheterna som utnyttjades för cyberattacker förra året blev kända redan 2024 eller tidigare. Det betonar vikten av att patcha system samt att byta lösenord och andra ID-uppgifter genast när en ny sårbarhet har avslöjats.

Mer information:

- Ladda ner hela 2026 Arctic Wolf Threat & Predictions Report.
- Diskutera med Arctic Wolf på Facebook, X, LinkedIn och YouTube.
- Besök arcticwolf.com och ta reda på mer om våra lösningar för operativ IT-säkerhet och slutpunkter.

Mediakontakt:

Fredrik Pallin
Digital PR
fredrik.pallin@digitalpr.dk

Om Arctic Wolf

Arctic Wolf är en global ledare inom operativ cybersäkerhet som hjälper företag att minska riskerna med cyberattacker. Arctic Wolfs molnbaserade säkerhetsplattform Aurora förenar kraften hos artificiell intelligens med världsledande säkerhetsexpertis för att erbjuda övervakning, motåtgärder och riskhantering dygnet runt. Vi får säkerhet att fungera!
www.arcticwolf.com