Pressmeddelande
26 februari 2025

Datastöld har blivit standard vid ransomware-attacker

Ny rapport visar hur hackarna har ändrat taktik. Vid 96 procent av alla ransomware-attacker förekommer nu datastöld. För att se över sin säkerhet betonar Arctic Wolf vikten av proaktiva åtgärder – fungerande backup och säkrare inloggning kan betyda mycket.

Arctic Wolf, ledande inom operativ IT-säkerhet, släpper nu sin årliga Threat Report som bygger på en ingående undersökning av det digitala hotlandskapet. Den nya rapporten visar hur cyberbrottslingar anpassar sina metoder för att kringgå förstärkta säkerhetsåtgärder. De prioriterar datastöld, utvecklar nya metoder för bedrägerier via e-post och utnyttjar kända sårbarheter för att genomföra intrång över hela världen.

Arctic Wolf Threat Report 2025 bygger på insikter från företagets uppdrag inom incidenthantering, hotanalyser samt data som samlats in genom företagets Aurora-plattform för säkerhetsövervakning. Det ger sammantaget en detaljerad bild av taktik, tekniker och metoder som angriparna använder för att ta sig genom cyberförsvaret.

I rapporten finns konkreta råd till organisationer som vill förbättra sin IT-säkerhet, utifrån analysen av den aktuella hotbilden. En god beredskap är ofta det bästa skyddet, inte minst fungerande backuprutiner. Enligt rapporten har backuper kunnat användas för återläsning av data i 68 procent av de undersökta fallen med ransomware-attacker.

– Vår nya Arctic Wolf Threat Report belyser en viktig förändring i hur hackarna går till väga: i dag är det mer regel än undantag att de stjäl data. Ransomware-attacker handlar inte längre bara om att låsa data genom kryptering. Hotaktörerna laddar först ner data för att öka pressen på de utsatta, säger Kerri Shafer-Page, chef för incidenthantering på Arctic Wolf.

Några slutsatser från 2025 Arctic Wolf Threat Report:

- **Först datastöld, sedan utpressning**. I takt med att företag har blivit bättre på att motstå ransomware-attacker och kan återstarta sina system genom backup väljer angriparna att stjäla data. Genom att hota med att läcka ut känsliga uppgifter ökar de pressen på sina offer. I 96% av de analyserade fallen med ransomware har datastöld förekommit.
- **Tre slags attacker dominerar.** Tre tillvägagångssätt svarar för 95% av alla fall av incidenthantering: ransomware (44%), bedrägeriförsök via e-post (27%) och intrång (24%). Många av de undersökta intrången som ser ut som misslyckade ransomware-attacker, men många sådana händelser handlar sannolikt om digitalt spionage där avsikten är att stjäla data.
- **Patcha säkerhetsluckor.** I 76 % av alla fall med intrång utnyttjade angriparna inte mer än 10 specifika sårbarheter – de flesta kopplade till verktyg för fjärruppkoppling och externa tjänster. Detta understryker behovet av proaktiv patchhantering.
- **Förhandling fungerar**. Arctic Wolf Incident Response Team hjälpte till att minska de sammanlagda kraven på lösensummor med 64%. 70% av kunderna som anlitade Arctic Wolfs förhandlingstjänster lyckades slippa betala lösen helt och hållet.
- **Lösenkrav vid ransomware: 6,4 Mkr**. Medianvärdet för begärd lösensumma ligger kvar på en hög nivå – 600 000 dollar (motsvarande 6,4 miljoner kr). Det visar att ransomware alltjämt är en lukrativ verksamhet för cyberbrottslingar.

- **Hotaktörerna följer pengarna**. E-post är en vanlig angreppsväg som fortsätter att växa, speciellt inom finans- och försäkringssektorn där phishing och andra e-postattacker svarar för 53% av de rapporterade incidenterna.

Att utnyttja sårbarheter i fjärranslutning via Remote Desktop Protocol (RDP) samt missbruk av användaruppgifter för VPN-uppkoppling är de vanligaste tillvägagångssätten vid ransomware-attacker och intrång. Det stora flertalet e-postattacker handlar om bedrägeri (phishing) eller möjliggörs av läckta användaruppgifter. Mer pålitlig identifiering och säkrare inloggningsmetoder som flerfaktorsautentisering är effektiva åtgärder för att stoppa sådana intrång.

Mer information:

- Ladda ner hela 2025 Arctic Wolf Threat 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.

Mediakontakt:

Fredrik Pallin
Digital PR
fredrik.pallin@digitalpr.dk

Om Arctic Wolf

Arctic Wolf är en global ledare inom operativ IT-säkerhet som hjälper företag och organisationer att minska riskerna med avancerade cyberattacker. Arctic Wolf tar med sin Aurora Platform varje vecka in och analyserar mer än 7 biljoner säkerhetshändelser vilket ger kunder i alla storlekar inom olika sektorer en bättre digital beredskap och uthållig motståndskraft.