

PRESSEMEDDELELSE

PRESSEMEDDELELSE - 485 procent flere ransomware rapporter i 2020

Pressemeddelelse · Udgivelse og medieindhold



Bitdefenders globale 2020 rapport om cybertrusler mod forbrugere er landet. Rapporten er baseret på Bitdefenders telemetri over indrapporterede trusler og sårbarheder og viser bl.a., hvordan truslen fra ransomware udviklede sig over året, en stigning i antallet af trusler mod Android-enheder i den anden halvdel af 2020, samt hvilke IoT-enheder der var de mest sårbare.

2020 var et år præget af corona-pandemien. Både når vi taler om almindelige menneskers liv, og når vi taler om udviklingen inden for trusler i cyberspace. I 2020 tilpassede cyberkriminelle nemlig deres kampagner og forsøgte at udnytte verdens ulykke til egen vinding. Herunder følger nedslag i rapportens vigtigste pointer, bl.a. udviklingen inden for ransomware-angreb, hvilke IoT-enheder de kriminelle går efter, samt hvilke der modtager

mest spam.

485 procent flere ransomware rapporter i 2020

Antallet af ransomware rapporter fra Windows-baserede enheder steg globalt med 485 procent i 2020 i forhold til 2019. Det lyder måske som et stort tal, men det er faktisk mindre end forventet. Årsagen til det lavere tal lader til at være, at ransomware-operatørerne i højere grad har rettet deres fokus mod større mål.

Ved at gå målrettet efter større ofre, som profitable virksomheder og velkendte organisationer, kan truslen om et nyt redskab de kriminelle tog i brug i 2020, afpresning, nemlig give bedre resultater. Ransomware-operatørerne er begyndt at true deres ofre med at offentliggøre særligt følsomme data, som de har fundet under deres angreb, hvis ikke ofrene betaler løsesummen.

Størstedelen af de globale ransomware-angreb fandt sted i løbet af 2020's første seks måneder. Det samme gælder angreb i Danmark, hvor henholdsvis første og andet kvartal oplevede 32 procent og 27 procent af årets samlede angreb.

En anden interessant udvikling, som Bitdefenders telemetri viser inden for trusler mod Windows-baserede enheder, er, at globale trusselsrapporter relateret til malwaren TrickBot faldt markant i løbet af 2020. TrickBot er en trojansk hest, der oftest er set brugt til at indsamle følsomme informationer og legitimationsoplysninger fra ofrenes enheder.

Malwaren indeholder også funktioner, der gør den i stand til at bevæge sig lateralt over kompromitterede netværk og inficere flere enheder. Det gør TrickBot til et populært redskab blandt cyberkriminelle. Faldet i antallet af angreb med TrickBot i løbet af 2020 er muligvis en konsekvens af, at TrickBots infrastruktur blev forsøgt lammet op til det amerikanske præsidentvalg.

Telemetrien viser omvendt en vækst i antallet af rapporter om de to andre trojanske heste, Emotet og AgentTesla, i den anden halvdel af 2020. Det kunne altså tyde på, at Emotet og AgentTesla udfyldte det tomrum som TrickBot efterlod.

32 procent flere trusler mod Android-enheder i anden halvdel af 2020

Sammenlignet med 2019, viser telemetrien en stigning i antallet af trusselsrapporter fra Android-enheder på 32 procent i anden halvdel af 2020. Over hele 2020 relaterede 35 procent af rapporterne sig til malware-familien Android.Trojan.Agent. Det er en type malware

der som regel skjuler sig på offerets enhed med det formål at indsamle oplysninger eller gøre enheden til en del af et botnet til DDoS-angreb (Distributed Denial of Service).

Den næstmest rapporterede malware-familie med 10 procent var Android.Trojan.Downloader, der som navnet antyder, bruges til at downloade andre typer malware på offerets enhed, efter at den er blevet kompromitteret.

92 procent af sårbare IoT-enheder bruger proprietære styresystemer

I 2020 steg antallet af trusler mod IoT-enheder. Mange mennesker tilbragte mere tid derhjemme, og der er sandsynligvis blevet købt flere smart-enheder som følge deraf.

Den mest sårbare type IoT-enhed, hvis man tæller på antallet af rapporterede sårbarheder, er NAS-enheder (Networked Attached Storage), der udgjorde 23 procent af den samlede mængde IoT-rapporter i 2020. Derudover steg antallet af identificerede sårbarheder hos NAS-enheder med 189 procent fra 2019 til 2020.

Medieafspillere stod for 19 procent af den samlede mængde rapporterede sårbarheder, mens smart TV'er og IP-kameraer (kameraer der kan kobles direkte på wifi-netværket) med 9 procent hver. Antallet af sårbarheder for Smart TV'er steg med 335 procent fra 2019 til 2020. For IP-kameraer var der tale om en stigning på 99 procent.

I 2020 var det mest fremtrædende styresystem på IoT-enheder iOS, der var på 37 procent af enhederne. Derefter kom proprietære systemer med 34 procent, Android og Windows med 10 procent hver og til sidst OSX med 5 procent.

Der tegner sig dog et andet billede, når vi ser på hvilke systemer, der blev rapporteret sårbarheder i; her udgør de proprietære systemer nemlig hele 92 procent.

Spam-kampagner udnyttede krisen

Globalt faldt mængden af spam mellem 2019 og 2020 med 3,88 procent. Dog er tallet steget med 4,5 procent i USA, sandsynligvis som følge af den økonomiske krise og almindelige menneskers ulykke, der potentielt gør dem mere sårbare over for at falde for de phishing-kampagner og svindelnumre, som cyberkriminelle står bag. Det kan f.eks. være tilbud om hurtige penge, som desperate folk, der er blevet fyret i ly af krisen, kan være mere tilbøjelige til at tro på.

USA tog førstepladsen som det land, der modtog mest spam, med 38 procent af den samlede mængde. Storbritannien indtog andenpladsen med syv procent og Sverige tredjepladsen med fem procent.

Spam-kampagner relateret til pandemien blev en fast del af trusselsbilledet i 2020. I det første halvår brugte de cyberkriminelle folks frygt og hungren efter viden om den nye virus til at snyde ofrene til enten at installere malware på deres enheder eller give personfølsomme oplysninger til bagmændene. I det andet halvår var de kriminelles motivation den samme, men i stedet for at bruge frygten som redskab, brugte de i stedet den økonomiske krise og dens konsekvenser.

Du kan læse Bitdefenders fulde rapport her:

<https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf>

Kilde / Logo / Foto: Bitdefender

Online: <https://pressemeddelelse.dk/pressemeddelelser/pressemeddelelse-485-procent-flere-ransomware-rapporter-i-2020/>

Pressemeddelelsen er videreformidlet af Pressemeddelelse.dk. Pressemeddelelse.dk er ikke ansvarlig for indholdet. Spørgsmål til indholdet rettes til Bitdefender.