RTL was slachtoffer ransomware-aanval, cybercriminelen maken 8500 euro buit

rtlnieuws.nl/nieuws/nederland/artikel/5255983/rtl-nederland-ransomware-aanval-cybercriminelen-losgeld

September 23, 2021

Bestanden versleuteld
23 september 2021 16:49 Aangepast: 23 september 2021 18:56

Het kantoor van RTL in Hilversum. Beeld © ANP

RTL Nederland is slachtoffer geworden van een ransomware-aanval. De cybercriminelen zijn de afgelopen tijd uit het netwerk gehaald en computers hersteld. RTL heeft uiteindelijk 8500 euro aan de aanvallers betaald.

Op donderdag 9 september ontdekte RTL een digitale aanval op zijn netwerk. Het bleek om ransomware te gaan: een aantal computers, servers en systemen binnen het Hilversumse kantoor van RTL werd gegijzeld door cybercriminelen en deels ontoegankelijk gemaakt.

Bestanden werden versleuteld

De aanvallers hebben toegang tot het netwerk van RTL gekregen doordat de inloggegevens van een medewerker van een externe beheerpartij zijn buitgemaakt. Deze partij beheert het netwerk van RTL. Er was geen dubbele beveiliging zoals tweestapsverificatie aanwezig, waardoor de aanvallers met de gestolen inloggegevens direct verregaande toegang op het netwerk kregen.

De aanvallers hebben toen de CryTOX-ransomware over het netwerk van RTL uitgerold. Bestanden werden versleuteld en op sommige computers verscheen een scherm met daarin het verzoek om losgeld te betalen. Ook een aantal belangrijke interne systemen, zoals het redactiesysteem van RTL Nieuws en het advertentieplanningssysteem, zijn door de ransomware platgelegd.

Een screenshot van de CryTOX-ransomware.

Direct aangifte gedaan

RTL heeft het Hilversumse netwerk geïsoleerd en de geïnfecteerde computers afgesloten van de rest, zodat de ransomware zich niet verder kon verspreiden. Daarna is gezocht naar de zogeheten patient zero: de plek waar de aanvallers binnen zijn gekomen. Dit gebeurde in samenwerking met technische partners zoals cybersecuritybedrijf Fox-IT en Infradata. Ook is er direct aangifte gedaan en de politie ingeschakeld.

De backups waren niet aangetast, waardoor RTL na de aanval direct is begonnen met het herstellen van geïnfecteerde systemen, zo vertelt RTL Nederland-cto Giovanni Piccirilli: "We hebben onmiddellijk besloten om onze systemen te isoleren om verdere aantasting te voorkomen. We hebben alles kunnen herbouwen met eigen schone back-upsystemen." De situatie was volgens Piccirilli binnen een 'aantal dagen' onder controle.

Lees ook:

RTL Nederland kampt met mogelijke ransomware-aanval

De systemen zijn in beveiligde omgevingen opgestart en mondjesmaat weer beschikbaar gemaakt. RTL Nieuws heeft bijna een week zonder redactiesysteem de uitzendingen gemaakt. Ook de bezoekers van de websites en apps hebben er niets van gemerkt. RTL benadrukt dat de consument geen last heeft gehad van de ransomware. Er is volgens RTL geen data gelekt of verlies geleden.

"We hebben de afgelopen jaren veel geïnvesteerd in beveiliging en awareness", zegt RTL Nederland-ceo Sven Sauvé. "Als een digitale aanval je dan toch overkomt, is het beste crisisplan de juiste professionals op de juiste plek, zodat je snel kunt handelen. Daarmee is de schade beperkt gebleven. Ik ben heel trots op ons team."

Bekijk deze video op RTL XL

Het is de nachtmerrie van elke ondernemer: hackers die je hele computersysteem platleggen met ransomware en vervolgens losgeld eisen. Het gebeurde ook bij automaterialenbedrijf Excluparts. "Ik denk dat dit voor veel bedrijven de doodsteek kan zijn."

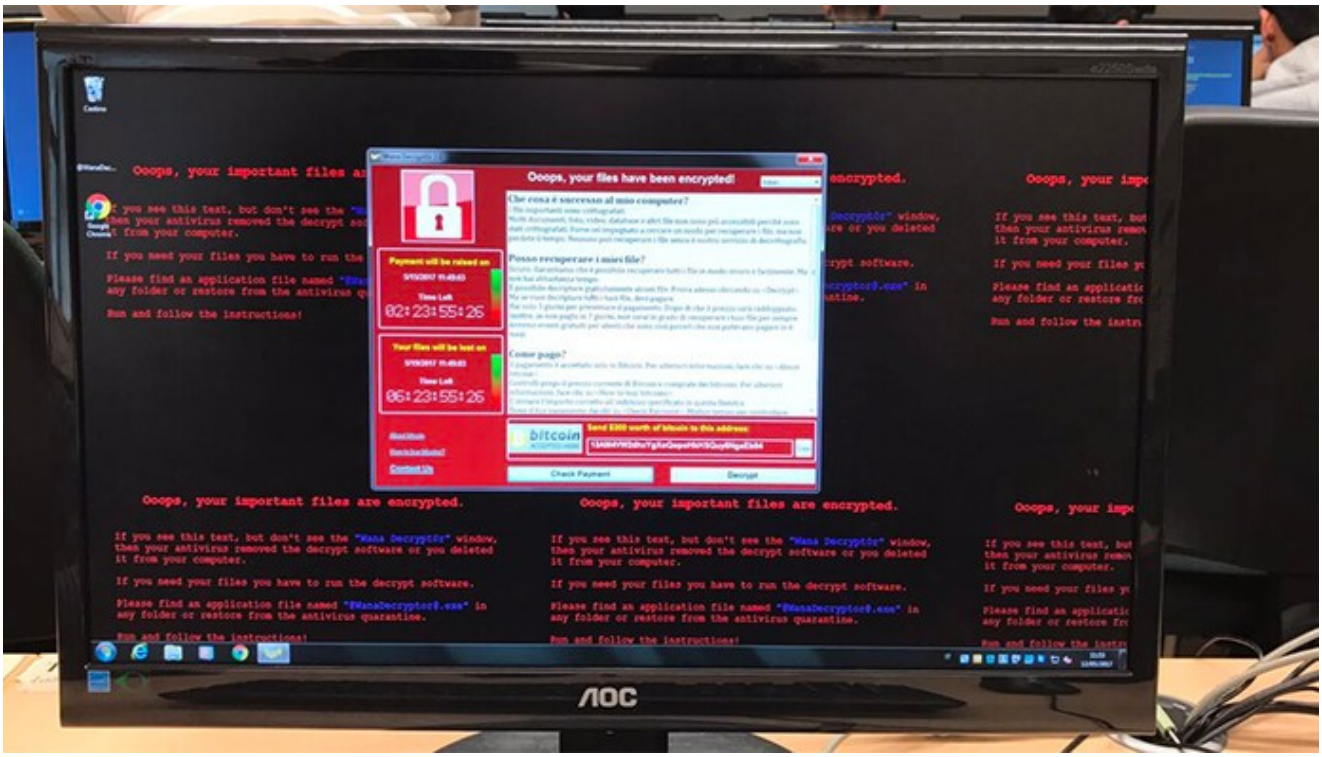
8500 euro betaald

RTL was de backups aan het herstellen maar heeft wel contact opgenomen met de cybercriminelen om te weten wat hun eisen waren. Het gebeurt vaker dat bedrijven in gesprek gaan met de aanvallers om te onderhandelen of tijd te rekken. De criminelen vroegen aan RTL 10.000 dollar, omgerekend zo'n 8500 euro, in bitcoin.

Dat is een verrassend laag bedrag, stelt Dave Maasland van cybersecuritybedrijf ESET Nederland: "Normaal gesproken worden er tonnen of miljoenen euro's aan losgeld gevraagd." Er kunnen allerlei verklaringen voor het lage bedrag zijn: misschien zagen de aanvallers dat de backups niet waren aangetast, proberen ze zo veel mogelijk geïnfecteerde bedrijven een klein bedrag te laten betalen, of waren de criminelen gewoonweg niet zo ervaren.

Betaling kan spoor nalaten

RTL heeft het bedrag betaald om eventuele opsporing mogelijk te maken, stelt het bedrijf. Bronnen binnen de opsporing bevestigen dat een bitcoinbetaling een spoor kan zijn naar de daders, omdat het geld op een gegeven moment moet worden opgenomen en uitgegeven. De nationale politie heeft als standpunt dat je nooit moet betalen, want dat houdt het verdienmodel van ransomware in stand.



Lees ook:

Justitie denkt aan verbod op betalen losgeld na aanval met ransomware