Fake DarkSide-campagne richt zich op energie- en voedselsectoren

Bedreigingsactoren achter een recente campagne doen zich voor als DarkSide in een poging om doelen te misleiden om losgeld te betalen.

Door: Cedric Pernet 18 juni 2021

De ransomware-aanval op het grote brandstofleveringsbedrijf Colonial Pipeline haalde onlangs de krantenkoppen. Het incident wordt toegeschreven aan de DarkSide-bedreigingsacteur, waardoor de naam van de groep opnieuw in de schijnwerpers komt te staan. Het zou dan ook niet verwonderlijk zijn dat dreigingsactoren misbruik maken van dit incident voor hun eigen sociaal ontworpen campagnes.

Verschillende bedrijven in de energie- en voedingsindustrie hebben onlangs dreigende e-mails ontvangen, zogenaamd van DarkSide. In deze e-mail beweert de dreigingsactor dat ze met succes het netwerk van het doelwit hebben gehackt en toegang hebben gekregen tot gevoelige informatie, die openbaar zal worden gemaakt als er geen losgeld van 100 bitcoins (BTC) wordt betaald.

De inhoud die in de e-mails wordt gebruikt, heeft ons echter doen geloven dat ze niet afkomstig waren van de genoemde bedreigingsgroep, maar van een opportunistische aanvaller op laag niveau die probeerde te profiteren van de huidige situatie rond DarkSide-ransomware-activiteiten.

De inhoud van de e-mails die in de campagne worden gebruikt

De e-mailcampagne begon op 4 juni en bereikte elke dag een paar doelen. E-mails met dreigende inhoud werden naar de generieke e-mailadressen van geselecteerde bedrijven gestuurd. Hier is een voorbeeld van de e-mailtekst:

Subject: Hacking [REDACTED: company name] servers

Hi, this is DarkSide.
It took us a lot of time to hack your servers and access all your accounting reporting. Also, we got access to many financial documents and other data that can greatly affect your reputation if we publish them. It was difficult, but luck was helped by us - one of your employees is extremely unqualified in network security issues. You could hear about us from the press - recently we held a successful attack on the JBS.
For non-disclosure of your confidential information, we require not so much - 100 bitcoins. Think about it, these documents may be interested not only by ordinary people, but also the tax service and other organizations, if they are in open access ... We are not going to wait long - you have several days.
Our bitcoin wallet – [REDACTED]

Afbeelding 1. Voorbeeldinhoud van de e-mail die is verzonden door dreigingsactoren die zich voordoen als DarkSide

De Bitcoin-portemonnee aan het einde van de e-mail is altijd hetzelfde voor elk doel. Op het moment van schrijven hebben de genoemde portefeuilles geen Bitcoin-betaling ontvangen of verzonden. Er is geen daadwerkelijke aanval terug te voeren op de e-mails en er zijn geen nieuwe doelen gesignaleerd.

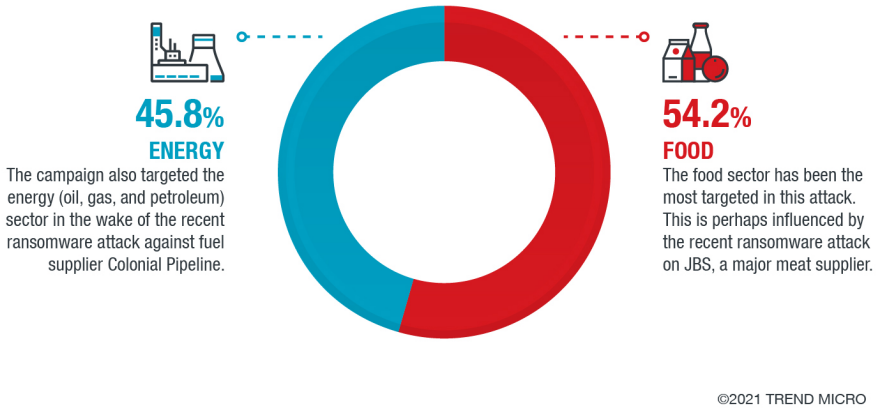
Meer dan alleen e-mails

Naast het sturen van gerichte e-mails naar bedrijven, kwamen we erachter dat dezelfde aanvaller ook contactformulieren heeft ingevuld op de websites van verschillende bedrijven.

De inhoud die via de webformulieren is verzonden, is dezelfde als die in de e-mails. In één geval konden we het IP-adres van de afzender achterhalen, 205[.]185[.]127[.]35, wat toevallig een Tor-netwerkuitgangsknooppunt is.

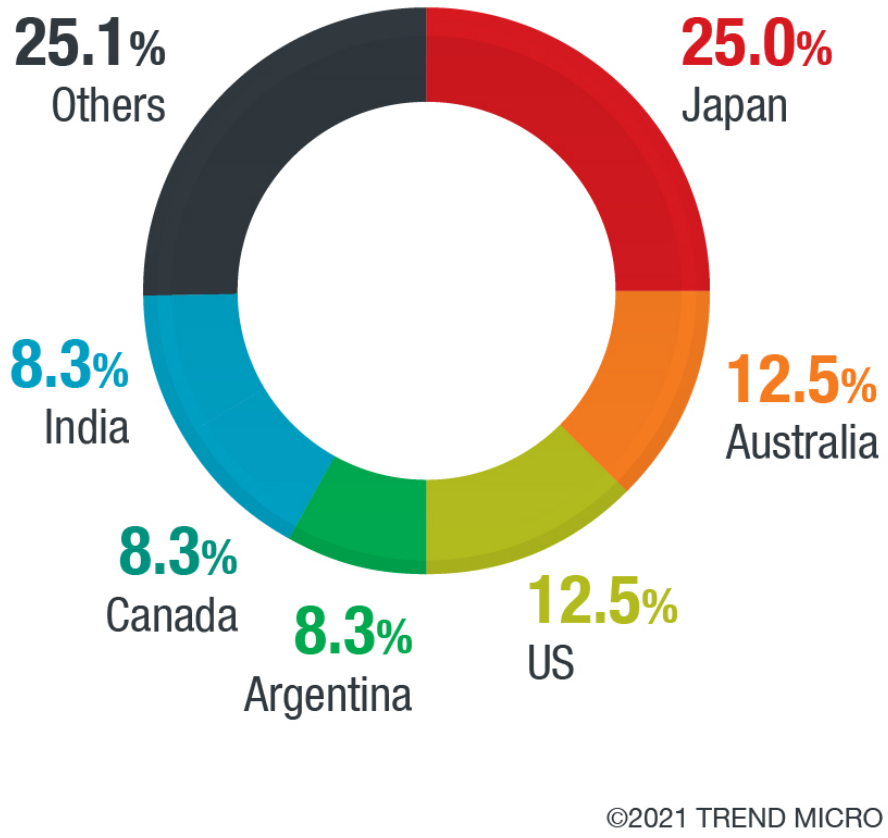
Energie- en voedingsindustrie als aantrekkelijke doelen

Op basis van de telemetriegegevens lijkt het erop dat de dreigingsactor alleen geïnteresseerd is in de energie (olie, gas en/of aardolie) en de voedingsindustrie; in feite behoren al hun doelstellingen tot deze sectoren.



Afbeelding 2. De sectoren waarop de nep-DarkSide-campagne is gericht

De campagne trof Japan het meest, gevolgd door verschillende andere landen: Australië, de VS, Argentinië, Canada, India. De overige getroffen landen zijn China, Colombia, Mexico, Nederland, Thailand en het VK.



Afbeelding 3. Landen die getroffen zijn door de nep-DarkSide-campagne

Tekenen dat dit geen echte DarkSide-campagne is

Het gedrag achter deze fraudecampagne is heel anders dan wat DarkSide vertoonde in zijn eerdere campagnes. DarkSide heeft altijd kunnen aantonen dat ze gestolen gevoelige gegevens hebben verkregen. Ze leiden hun doelwitten ook naar een website die wordt gehost op het Tor-netwerk. In deze campagne vermeldt de e-mail echter niets over het bewijs dat ze inderdaad vertrouwelijke of gevoelige informatie hebben verkregen.

Ook lanceerde DarkSide , net als de meeste moderne ransomware-aanvallen , de ransomware om de activiteiten van hun doelwit te verlammen voordat er losgeld werd geëist. Hier is er geen codering van inhoud op het doelnetwerk; de acteurs sturen gewoon een dreigement en een losgeldeis op basis van de bewering dat ze naar verluidt de gegevens hebben.

Misschien wel het meest veelzeggende: de actoren achter deze bedreigingen noemden JBS als het slachtoffer van een van hun recente gepubliceerde aanvallen; de JBS-aanval werd niet toegeschreven aan DarkSide, maar aan REvil (ook bekend als Sodinokibi).

Al met al ziet deze campagne er amateuristisch uit in vergelijking met bekende eerdere DarkSide-activiteiten. Het gevraagde bedrag van elk doelwit, 100 BTC, is ongeveer 4 miljoen dollar waard. We zijn van mening dat de meeste bedrijven niet zullen worden aangespoord om dat bedrag te betalen zonder enig echt bewijs dat het netwerk is gecompromitteerd en dat gevoelige gegevens op het punt staan in het openbaar te lekken.

Waarom richten ze zich op essentiële sectoren?

Hoewel de rest van de campagne onhandige technieken laat zien, is het vermeldenswaard dat de aanvaller met een reden bewust bedrijven in specifieke sectoren heeft geselecteerd. De beslissing om deze doelen met de hand te kiezen, wordt waarschijnlijk beïnvloed door de recente ransomware-aanvallen op JBS en Colonial Pipeline , die tot dezelfde bedrijfstakken behoren.

Deze bedrijfstakken zijn niet alleen getroffen door deze recente aanvallen, maar zijn in het verleden ook consequent tot de meest doelwitten geweest. In ons rapport over cyberbeveiliging in 2020 vonden we de voedsel- en drankenindustrie en de olie- en gasindustrie in de top tien van industrieën die het meest het doelwit waren van ransomware.

Een van de oorzaken hiervan kan zijn dat van deze sectoren wordt verwacht dat ze dagelijks essentiële goederen en/of diensten leveren. Hoe langer de aanval niet wordt gedwarsboomd en de bedrijfsactiviteiten vervolgens worden onderbroken, hoe meer de getroffen organisatie winst en reputatie verliest. De sluiting van deze diensten kan ook publieke opschudding en paniek veroorzaken, vooral wanneer het mogelijk een groot aantal mensen treft.

In de nasleep kan de impact van een aanval de angst voor voedsel- en/of energiezekerheid doen toenemen , wat paniekaankopen kan veroorzaken, aangezien het publiek zich zorgen maakt over mogelijke prijsstijgingen die door de aanval kunnen worden veroorzaakt.

Dit is een van de redenen waarom aanvallers, zowel echt als nep, ervoor zouden kiezen om campagnes te lanceren op essentiële leveranciers: hun doelwitten zijn zich bewust van de verstrekkende onmiddellijke effecten die een aanval kan hebben, niet alleen voor het bedrijf zelf, maar ook voor ook van consumenten. Als we dit in overweging nemen, is de kans groter dat de doelen toegeven aan de losgeldeisen. In de campagne die we zagen, heeft gelukkig niemand daadwerkelijk betaald, waarschijnlijk vanwege de twijfelachtige details in de e-mail. Dit neemt echter niet de mogelijkheid weg dat een aanvaller met meer geloofwaardige methoden met succes doelen kan verstrikken.

In het kielzog van de angst die werd veroorzaakt door recente ransomware-aanvallen die grote bedrijven troffen, moeten organisaties altijd de geldigheid van de bedreigingen verifiëren voordat ze actie ondernemen. Sterker nog, organisaties kunnen deze bedreigingen uit de kiem smoren door beveiligingsoplossingen te gebruiken die spam en andere op e-mail gebaseerde bedreigingen blokkeren.