Aanvallen gericht op zorgorganisaties nemen wereldwijd toe naarmate COVID-19-gevallen weer toenemen

Eind oktober 2020 meldden we dat ziekenhuizen en zorginstellingen het doelwit waren van een toenemende golf van ransomware-aanvallen, waarbij de meeste aanvallen gebruik maakten van de beruchte Ryuk- ransomware. Dit volgde op een gezamenlijk cybersecurity-advies van de CISA, FBI en HHS, waarin werd gewaarschuwd voor een toenemende en onmiddellijke cybercriminaliteitsdreiging voor Amerikaanse ziekenhuizen en zorgverleners.

Helaas is die dreiging van cybercriminaliteit de afgelopen twee maanden verergerd. Sinds begin november is het aantal aanvallen op gezondheidsorganisaties wereldwijd met 45% toegenomen. Dit is meer dan het dubbele van de totale toename van cyberaanvallen in alle industriesectoren wereldwijd in dezelfde periode.

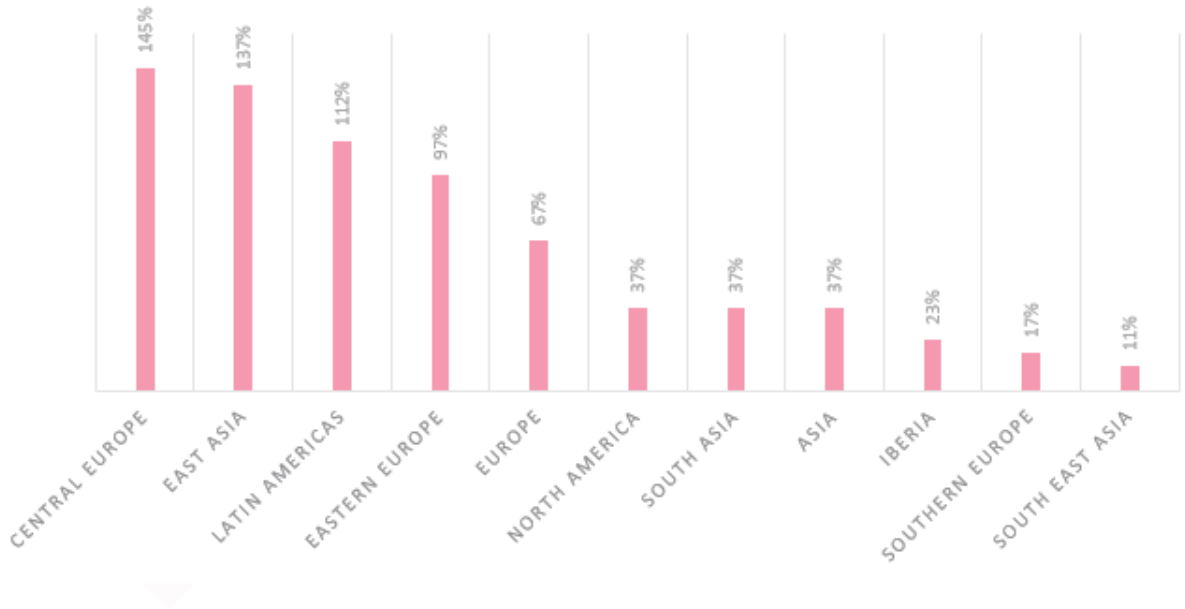
De toename van het aantal aanvallen heeft betrekking op een reeks vectoren, waaronder ransomware, botnets, uitvoering van externe code en DDoS-aanvallen. Ransomware vertoont echter de grootste toename en vormt de grootste malwarebedreiging voor zorgorganisaties in vergelijking met andere bedrijfstakken. Ransomwareaanvallen op ziekenhuizen en aanverwante organisaties zijn bijzonder schadelijk, omdat elke verstoring van hun systemen hun vermogen om zorg te verlenen kan aantasten en het leven in gevaar kan brengen - dit alles wordt nog verergerd door de druk waarmee deze systemen worden geconfronteerd bij het omgaan met de wereldwijde toename van COVID-19. gevallen. Dit is precies de reden waarom criminelen zich specifiek en hardvochtig richten op de gezondheidszorg: omdat ze denken dat ziekenhuizen eerder geneigd zijn om aan hun losgeldeisen te voldoen.

Globaal overzicht van aanvallen

- Aangezien de november 1 st , 2020 is er een toename van meer dan 45% van het aantal aanvallen gezien tegen zorginstellingen wereldwijd geweest, in vergelijking met een gemiddelde stijging 22% aanvallen op andere bedrijfstakken.
- Het gemiddelde aantal wekelijkse aanvallen in de zorgsector bedroeg in november 626 per organisatie, tegen 430 in oktober.
- Aanvallen met ransomware, botnets, uitvoering van externe code en DDoS namen allemaal toe in november, waarbij ransomwareaanvallen de grootste piek vertoonden in vergelijking met andere bedrijfstakken.
- De belangrijkste ransomwarevariant die bij aanvallen wordt gebruikt , is Ryuk , gevolgd door Sodinokibi .

Regionale aanvalsgegevens

Centraal-Europa staat bovenaan de lijst van regio's die getroffen zijn door de piek in aanvallen op gezondheidsorganisaties, met een stijging van 145% in november, gevolgd door Oost-Azië, met een stijging van 137%, en Latijns-Amerika met een stijging van 112%. Europa en Noord-Amerika kenden een stijging van respectievelijk 67% en 37%.



MEER AANVALLEN, PER GEZONDHEIDSORGANISATIE, PER REGIO

Wat specifieke landen betreft, kende Canada de meest dramatische toename met meer dan 250% toename van het aantal aanvallen, gevolgd door Duitsland met een stijging van 220%. Spanje zag een verdubbeling van het aantal aanvallen.

Waarom nemen de aanvallen nu toe?

De belangrijkste motivatie voor dreigingsactoren met deze aanvallen is financieel. Ze zijn op zoek naar grote bedragen, en snel. Het lijkt erop dat deze aanvallen het afgelopen jaar zeer goed hebben beloond voor de criminelen achter hen, en door dit succes hebben ze honger naar meer.

Zoals we eerder hebben aangestipt, staan ziekenhuizen onder enorme druk als gevolg van de aanhoudende stijging van het aantal gevallen van coronavirus en zijn ze bereid losgeld te betalen zodat ze in deze kritieke tijd zorg kunnen blijven bieden. In september werd door de Duitse autoriteiten gemeld dat wat een verkeerd gerichte hackeraanval lijkt te zijn geweest, de uitval

veroorzaakte van IT-systemen in een groot ziekenhuis in Düsseldorf, en een vrouw die dringend moest worden opgenomen stierf nadat ze voor behandeling naar een andere stad moest worden gebracht. . Geen enkel ziekenhuis of zorginstelling zou een soortgelijk scenario willen meemaken, waardoor de kans groter wordt dat de organisatie voldoet aan de eisen van de aanvaller in de hoop de verstoring tot een minimum te beperken.

Het is ook belangrijk op te merken dat, in tegenstelling tot gewone ransomwareaanvallen, die op grote schaal worden verspreid via massale spamcampagnes en exploitkits , de aanvallen op ziekenhuizen en zorginstellingen die de Ryuk- variant gebruiken, specifiek op maat en gericht zijn. Ryuk werd voor het eerst ontdekt in midden 2018, en kort daarna, Check Point Research publiceerde de eerste grondige analyse van deze nieuwe Ransomware, die de Verenigde Staten werd gericht. In 2020 volgden Check Point-onderzoekers van CPR de Ryuk-activiteit wereldwijd en observeerden ze de toename van het gebruik van Ryuk bij aanvallen gericht op de gezondheidszorg.

Het cyberlandschap van COVID-19

De pandemie heeft elk aspect van ons leven aangetast en het cyberveiligheidslandschap is niet gespaard gebleven. Van een toename in de registratie van coronavirus-gerelateerde kwaadaardige domeinen, tot het gebruik van gerelateerde onderwerpen bij phishing- en ransomware-aanvallen, en zelfs fraudeadvertenties die Covid-vaccins te koop aanbieden, we hebben een ongekende toename gezien van cyber-exploits om persoonlijke gegevens in gevaar te brengen. , malware verspreiden en geld stelen.

Medische diensten en onderzoeksorganisaties werden het doelwit van aanvallen om waardevolle commerciële en professionele informatie te stelen of om essentiële onderzoeksactiviteiten te verstoren. Het gebruik van test- en trace-apps voor het volgen van personen, wat voorheen tot sterke privacygerelateerde tegenstand zou hebben geleid, wordt wereldwijd op grote

schaal toegepast en zal naar verwachting de pandemie overleven. Terwijl de aandacht van de wereld blijft focussen op het aanpakken van de pandemie, zullen cybercriminelen die focus ook blijven gebruiken en proberen te exploiteren voor hun eigen illegale doeleinden - het is dus essentieel dat zowel organisaties als individuen een goede cyberhygiëne handhaven om zichzelf te beschermen. tegen Covid-gerelateerde online criminaliteit.

Tips om ransomware en phishingaanvallen te voorkomen

1. **Zoek naar trojan-infecties - ransomware-aanvallen beginnen niet met ransomware** . Ryuk en andere soorten ransomware-exploits beginnen meestal met een eerste infectie met een trojan. Vaak vindt deze trojan-infectie plaats dagen of weken voordat de ransomwareaanval begint, dus beveiligingsprofessionals moeten uitkijken naar **Trickbot-, Emotet-, Dridex- en Cobalt Strike-** infecties binnen hun netwerken en deze verwijderen met behulp van oplossingen voor het opsporen van bedreigingen - aangezien deze allemaal de deur voor Ryuk kunnen openen .
2. **Houd uw hoede voor het weekend en op feestdagen** - de meeste ransomwareaanvallen van het afgelopen jaar vonden plaats in het weekend en tijdens vakanties, wanneer IT- en beveiligingspersoneel minder snel aan het werk zijn.
3. **Gebruik anti-ransomware-** oplossingen - hoewel ransomware-aanvallen geavanceerd zijn, zijn **anti-ransomware** - oplossingen met een herstelfunctie effectieve hulpmiddelen waarmee organisaties binnen enkele minuten kunnen terugkeren naar hun normale werking als er een infectie plaatsvindt.

4. **Voorlichting van werknemers over kwaadaardige e-mails** - Het is van cruciaal belang om gebruikers te trainen in het identificeren en vermijden van mogelijke ransomwareaanvallen. Veel van de huidige cyberaanvallen beginnen met een gerichte phishing-e-mail die niet eens malware bevat, maar alleen een sociaal ontworpen bericht dat de gebruiker aanmoedigt om op een kwaadaardige link te klikken of om specifieke details te verstrekken. Gebruikerseducatie om dit soort kwaadaardige e-mails te helpen identificeren, wordt vaak beschouwd als een van de belangrijkste verdedigingsmechanismen die een organisatie kan inzetten.

5. **Virtuele patching** - de federale aanbeveling is om oude versies van software of systemen te patchen, wat voor ziekenhuizen onmogelijk zou kunnen zijn, aangezien systemen in veel gevallen niet kunnen worden gepatcht. Daarom raden we het gebruik van een Intrusion Prevention System (IPS) met virtuele patchfunctie aan om pogingen om zwakke punten in kwetsbare systemen of applicaties te misbruiken te voorkomen. Een bijgewerkte IPS helpt uw organisatie beschermd te blijven.