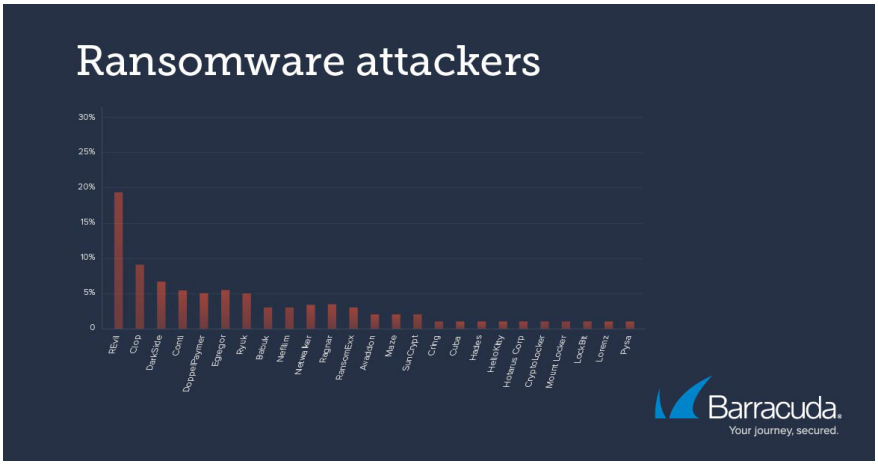
Threat Spotlight: Trends op het gebied van ransomware

14 augustus, 2021 | Fleming Shi

Ransomware-aanvallen hebben in 2021 een vlucht genomen: het aantal aanvallen is drastisch gestegen en de bedragen die aan losgeld worden betaald, blijven de pan uit rijzen. Cybercriminelen hebben steeds meer doelwitten: hun aandacht verschuift naar onze kritieke infrastructuur en ontwikkelt zich in diepgewortelde supply chain attacks die langdurige schade kunnen aanrichten.

De grimmige vooruitzichten voor de toekomst van ransomware zijn meedogenloos. Niemand wordt gespaard voor financiële schade of merkverwoestende krantenkoppen. Ransomware-criminelen hebben hun weg gevonden naar het fundament van onze digitale economie, van vertrouwde softwareleveranciers tot IT-dienstverleners.

Veel van deze aanvallen worden geleid door een handvol prominente ransomware-bendes. Uit onze analyse van ransomware-aanvallen die tussen augustus 2020 en juli 2021 plaatsvonden, blijkt dat REvil verantwoordelijk was voor 19% van de aanvallen en DarkSide voor 8%.



Ransomware-aanvallers

In deze editie van Threat Spotlight kijken we naar de ransomware-aanvalspatronen die we hebben geïdentificeerd in onze analyse van aanvallen die de afgelopen 12 maanden plaatsvonden en delen we onze inzichten op het gebied van preventie en recovery.

De dreiging

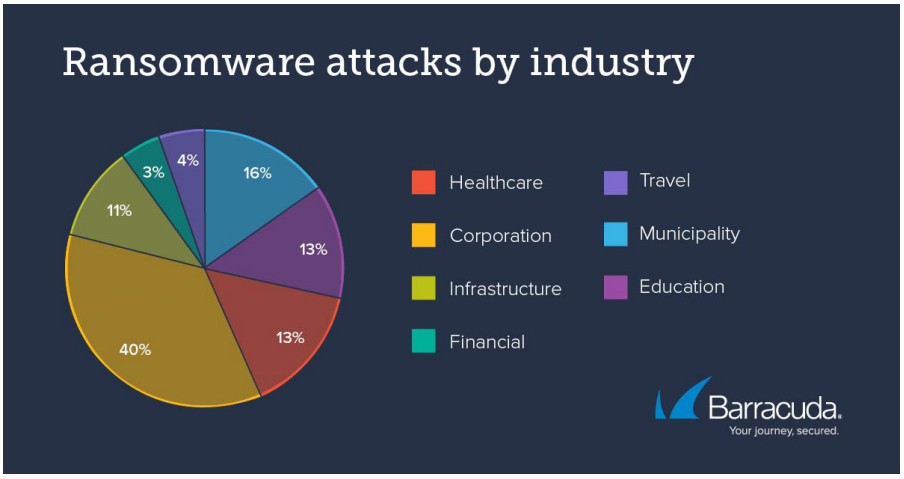
Ransomware - Cybercriminelen gebruiken kwaadaardige software, vaak vermomd in de vorm van een e-mailbijlage of hyperlink, om het netwerk te infiltreren en e-mails, gegevens en andere kritieke bestanden te vergrendelen tot er losgeld is betaald. Deze evoluerende en geraffineerde aanvallen zijn schadelijk en kostbaar. Ze kunnen de dagelijkse werkzaamheden stilleggen, chaos veroorzaken en tot financiële verliezen leiden als gevolg van downtime, losgeldbetalingen, herstelkosten en andere onvoorziene, niet-gebudgetteerde uitgaven.

Onlangs hebben criminelen hun tactieken verfijnd tot een dubbele afpersingsconstructie. Ze baseren hun losgeldeisen op onderzoek dat ze voor de aanval uitvoeren. Vervolgens stelen ze gevoelige informatie van hun slachtoffers en eisen ze een betaling in ruil voor de belofte dat deze informatie niet openbaar wordt gemaakt of aan andere criminelen wordt verkocht. Omdat criminelen niet te vertrouwen zijn, worden slachtoffers die betalen vaak na enkele maanden weer gecontacteerd en opnieuw om een betaling gevraagd om de gestolen gegevens geheim te houden. Sommige ransomware-criminelen nemen het geld aan, maar verkopen de gestolen gegevens daarna alsnog.

De details

In de afgelopen twaalf maanden hebben onderzoekers van Barracuda 121 ransomware-incidenten geïdentificeerd en geanalyseerd, een toename van 64 procent ten opzichte van het jaar ervoor. Cybercriminelen richten zich nog steeds in het bijzonder op gemeentes, gezondheidszorg en onderwijs, maar ook aanvallen op andere organisaties nemen toe.

Aanvallen op bedrijven in sectoren zoals infrastructuur, reizen, financiële dienstverlening en meer vormden tussen augustus 2020 en juli 2021 in totaal 57 procent van alle ransomware-aanvallen, een stijging ten opzichte van 18 procent in ons onderzoek van vorig jaar. Infrastructuur-gerelateerde bedrijven waren doelwit van 11 procent van de aanvallen die we onderzochten. Ransomware-aanvallen evolueren snel tot software supply chain attacks, zodat er meerdere bedrijven in één keer kunnen worden geraakt.



Ransomware-aanvallen per branche

We hebben eerder beschreven hoe gemeentes niet altijd goed zijn voorbereid op dit soort aanvallen, vaak als gevolg van krappe budgetten, weinig IT-personeel en verouderde tools. Maar het probleem is veel erger dan we dachten, zeker nu vertrouwde softwareleveranciers een risico zijn geworden voor hun eigen klanten. Het aantal aanvallen uit onverwachte bronnen neemt alarmerend snel toe.

Hoewel cybercriminelen hun ransomware-aanvallen nog altijd voornamelijk richten op organisaties in de Verenigde Staten, blijkt uit ons onderzoek dat ransomware-aanvallen steeds meer wijdverspreid worden. Iets minder dan de helft van de aanvallen in de afgelopen 12 maanden was gericht op Amerikaanse organisaties (44 procent). Ter vergelijking: 30 procent van de incidenten vond plaats in EMEA, 11 procent in Zuidoost-Aziatische landen, 10 procent in Zuid-Amerika en 8 procent in Canada en Mexico.

Ransomware-aanvallen per land

Exploiteren van applicatiekwetsbaarheden in ransomware-aanvallen.

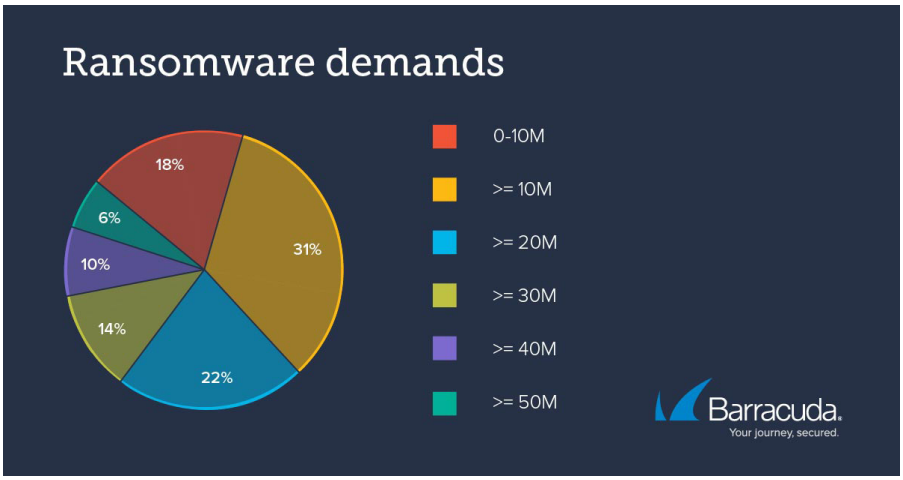
De patronen van ransomware-aanvallen evolueren ook. In plaats van simpelweg te vertrouwen op kwaadaardige hyperlinks en e-mailbijlagen voor de verspreiding van ransomware, hebben cybercriminelen hun tactieken verfijnd. Eerst proberen aanvallers een manier te vinden om inloggegevens te stelen via phishing-aanvallen, waarna ze de gestolen informatie gebruiken om de webapplicaties van het slachtoffer te infiltreren. Als een applicatie eenmaal is gecompromitteerd, kan de aanvaller ransomware en andere malware in het systeem introduceren. Hierdoor kan zowel uw netwerk als dat van de gebruikers van uw applicatie geïnfecteerd worden.

Het is belangrijk om op te merken dat webapplicaties veel verschillende vormen hebben, ook om bijvoorbeeld thuiswerken te accommoderen. Een webportaal voor een gedeelte van uw IT-infrastructuur is net zo gevaarlijk als een uitgebreide SaaS-applicatie. Het afgelopen jaar hebben aanvallers meerdere keren applicatiekwetsbaarheden geëxploiteerd om controle te krijgen over de applicatie-infrastructuur, zodat de meest waardevolle gegevens versleuteld konden worden.

De top 10 dreigingen van de OWASP op het gebied van applicatiebeveiliging zijn allemaal mogelijke mechanismen om toegang te krijgen tot de infrastructuur van een organisatie. Enkel op een VPN vertrouwen voor het accommoderen van thuiswerkers creëert aanzienlijke risico's, omdat veel inloggegevens bekend zijn op het darkweb door gelekte wachtwoorden. Zo kon de ransomware-aanval die leidde tot de langdurige uitval van de Colonial-pijpleiding in mei bijvoorbeeld worden uitgevoerd doordat hackers toegang tot het netwerk hadden via een VPN-account, waarvan zij het wachtwoord hadden verkregen via het darkweb.

Trends op het gebied van losgeldbetalingen

Zoals we de afgelopen jaren hebben gezien, zijn de losgeldbedragen die worden gevraagd steeds hoger geworden. Gemiddeld wordt er per incident nu meer dan 10 miljoen dollar aan losgeld geëist. In slechts 18 procent van de incidenten was de losgeldeis lager dan 10 miljoen dollar; in 30 procent van de incidenten was deze hoger dan 30 miljoen dollar.



Losgeldeisen

De toenemende populariteit van cryptovaluta heeft geleid tot een toename van het aantal ransomware-aanvallen en hogere losgeldeisen. Nu het steeds eenvoudiger wordt om Bitcoin-transacties te traceren, bieden criminelen vaak alternatieve betaalmethoden aan. Zo vraagt de ransomeware-groep REvil om betaling in Monero in plaats van Bitcoin.

In ons onderzoek kwamen we echter ook meerdere voorbeelden tegen waarin slachtoffers het geëiste losgeldbedrag wisten te verlagen door hierover te onderhandelen. Zo wist JBS de losgeldeis van 22,5 miljoen dollar te verlagen tot 11 miljoen dollar, en Brenntag, een distributeur van chemische stoffen uit Duitsland, van 7,5 miljoen dollar tot 4,4 miljoen dollar. De initiële losgeldeis is vaak niet definitief. Is een slachtoffer van ransomware bereid om te betalen, dan is het belangrijk om onderhandelingsopties te verkennen. Het resultaat kan oplopen tot miljoenen aan besparingen.

Steeds meer organisaties weigeren daarentegen om losgeld te betalen, wat waarschijnlijk bijdraagt aan de hoge initiële losgeldeisen. Deze trend wordt ook gevolgd door meer samenwerking met de autoriteiten en losgeldonderhandelaars. De FBI heeft onlangs de Bitcoin-wallets van DarkSide gelokaliseerd en wist een deel van de losgeldbetalingen terug te krijgen. Ook hebben de autoriteiten betalingen aan partners van de ransomwaregroep geblokkeerd.

Het zijn bemoedigende ontwikkelingen in het gevecht tegen deze cyberaanvallen. Naast juridische actie, hebben we ook gezien hoe het Witte Huis zich rechtstreeks tot andere wereldleiders heeft gericht en harde maatregelen eiste tegen het onderbrengen van cybercriminelen. Gezien de spraakmakende effecten en grote impact van recente aanvallen, met name die op kritieke infrastructuur, geloof ik dat de Amerikaanse regering zich niet langer alleen tot waarschuwen zal beperken. Men is bereid om serieus actie te ondernemen, zelfs tegen natiestaten, als er duidelijk bewijs is van medeplichtigheid of nalatigheid bij het optreden tegen cybercriminelen.

Zo beschermt u zich tegen ransomware

- **De eerste stap in het gevecht tegen ransomware is aannemen dat u vroeger of later zelf slachtoffer zult worden.** Daarna moet u zich tot doel stellen om geen losgeld te betalen. Met dat doel dient u in elk geval de volgende drie procedures te implementeren om dit te bereiken.
- **Doe al het mogelijke om verlies van inloggegevens te voorkomen**. Implementeer anti-phishing-beveiligingen in e-mail- en andere samenwerkingsprogramma's en werk voortdurend aan het bewustzijn van uw gebruikers op het gebied van e-mailbeveiliging. Beveilig uw applicaties en toegang. Naast het gebruik van MFA dient u ook webapplicatiebeveiligingen te implementeren voor al uw SaaS-toepassingen en infrastructuur-toegangspunten.

Applicatiekwetsbaarheden blijven vaak verborgen in de applicatiecode of onderliggende applicatie-infrastructuur. Bescherm uw applicaties daarom tegen de top 10 dreigingen van de OWASP. Als u API-interacties hebt in uw applicatie, dient u er tevens voor te zorgen dat u tegen de top 10 API-dreigingen van de OWASP bent beschermd. Naast het beschermen van uw applicaties moet u proberen om, waar mogelijk, de toegang die u aan uw gebruikers geeft te beperken. Probeer als het kan om altijd de minst mogelijke toegang aan uw gebruikers te geven die zij nodig hebben om productief te werken. De beste oplossing is het implementeren van Zero Trust Access op basis van eindpuntbeveiligingen.

- **Maak een back-up van uw gegevens**. Blijf up-to-date met een veilige oplossing voor gegevensbescherming die uw kritieke informatie-activa kan identificeren en implementeer respons- en herstelmogelijkheden. Zo weet u dat u altijd nee kunt zeggen tegen ransomware-criminelen.

Cybercriminelen willen steeds grotere winsten maken. Daarom moet de beveiligingsindustrie oplossingen blijven ontwikkelen die voor bedrijven van elke omvang gemakkelijk te gebruiken zijn. Aanvallers beginnen vaak bij kleine organisaties die zijn aangesloten op de grotere doelen, en werken daarvandaan omhoog. Ik hoop dat we allemaal producten kunnen maken die goed samenwerken. Als producten te ingewikkeld zijn voor een bepaald marktsegment, moeten we geavanceerde technologie en producten omzetten in diensten die kunnen worden geconsumeerd zonder dure en schaarse beveiligingstalenten.

Fleming Shi

Fleming Shi is Chief Technology Officer bij Barracuda, waar hij leiding geeft aan de teams die onderzoek doen naar dreigingen en innovaties voor het bouwen van toekomstbestendige technologieplatforms. Hij heeft meer dan 20 patenten op het gebied van netwerk- en contentbeveiliging op zijn naam staan.