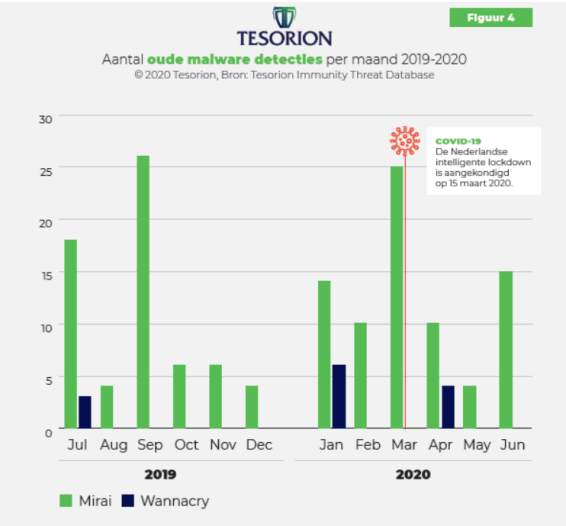
Oude malware-varianten WannaCry en Mirai-botnet blijven bedreiging

Organisaties verzuimen tijdig en adequaat te patchen

Leusden – Malware van zo'n drie jaar geleden, zoals de ransomware-variant WannaCry en het Mirai-botnet, blijken nog altijd schade aan te richten. Dit concludeert cybersecurity organisatie Tesorion uit eigen onderzoek. Ondanks dat deze vormen van malware al geruime tijd geleden zijn ontmaskerd, worden deze nog regelmatig gedetecteerd door Tesorion Immunity. Dit betekent dat organisaties onnodig gevaar blijven lopen op een denial-of-service- of ransomware-aanval.

Wie had verwacht dat de rol van het Mirai-botnet en het WannaCry-virus na hun ontmaskering in respectievelijk 2016 en 2017 was uitgespeeld, komt bedrogen uit. Op bedrijfsnetwerken bewaakt door Tesorion werden deze oude vormen van malware vele tientallen keren waargenomen tussen juli 2019 en juni 2020. Met een piek tijdens de start van het nieuwe schooljaar in 2019 én bij het uitbreken van de coronacrisis.



Mirai

Mirai werkt vooral op IoT-apparaten, zoals videocamera's en routers voor thuisgebruik. In september 2016 werden grote hoeveelheden geïnfecteerde apparaten ingezet om een grootschalige en gerichte denial-of-service-aanval te lanceren. Het probleem is dat deze apparaten lastig te patchen zijn en uit de cijfers blijkt dat talloze organisaties hier niet (goed) op gereageerd hebben.

WannaCry
De WannaCry ransomware heeft in 2017 ongekende schade aangericht bij grote bedrijven zoals Renault, National Health Service, Q-Park, Deutsche Bahn en meer. Hoewel een Windows-patch al geruime tijd beschikbaar was, bleken deze organisaties toch te laat. Zelfs vandaag de dag worden nog altijd geïnfecteerde systemen aangetroffen.

Patchen, patchen, patchen
Ernst Veen, product manager bij Tesorion: “We zijn erg geschrokken van het feit dat we nog relatief veel oude malware-infecties detecteren. Dit geeft aan dat organisaties hun patch-beleid nog altijd niet op orde hebben. Ondanks het feit dat Mirai en WannaCry al jaren terug zijn ontdekt, kunnen zij nog altijd veel schade aanrichten. We blijven erop hameren dat organisaties hun software up-to-date houden. Mocht een apparaat niet gepatcht kunnen worden, zoals een beveiligingscamera, zorg dan dat dit apparaat vervangen wordt. Tegelijkertijd raden wij aan om regelmatig back-ups te maken en het netwerk te segmenteren. Mochten er dan toch security-incidenten plaatsvinden, dan kun je deze eenvoudig isoleren en blijft de schade beperkt.”

Meer weten over hoe malware bestreden kan worden? Lees ons onderzoeksrapport.

Over Tesorion
Tesorion helpt organisaties het hoofd te bieden aan de meest uiteenlopende vormen van cybercriminaliteit. De diensten variëren van het vergroten van awareness, tot het bieden met mitigerende oplossingen, digitaal forensisch onderzoek of het bieden van nazorg na een digitale inbraak. Tesorion is een Nederlandse cybersecurity expert met 160 experts, is een associate partner van het NoMoreRansom project en is door Microsoft genoemd als ‘Threat Indicator Top Contributor’. Meer informatie is te vinden op: https://www.tesorion.nl/