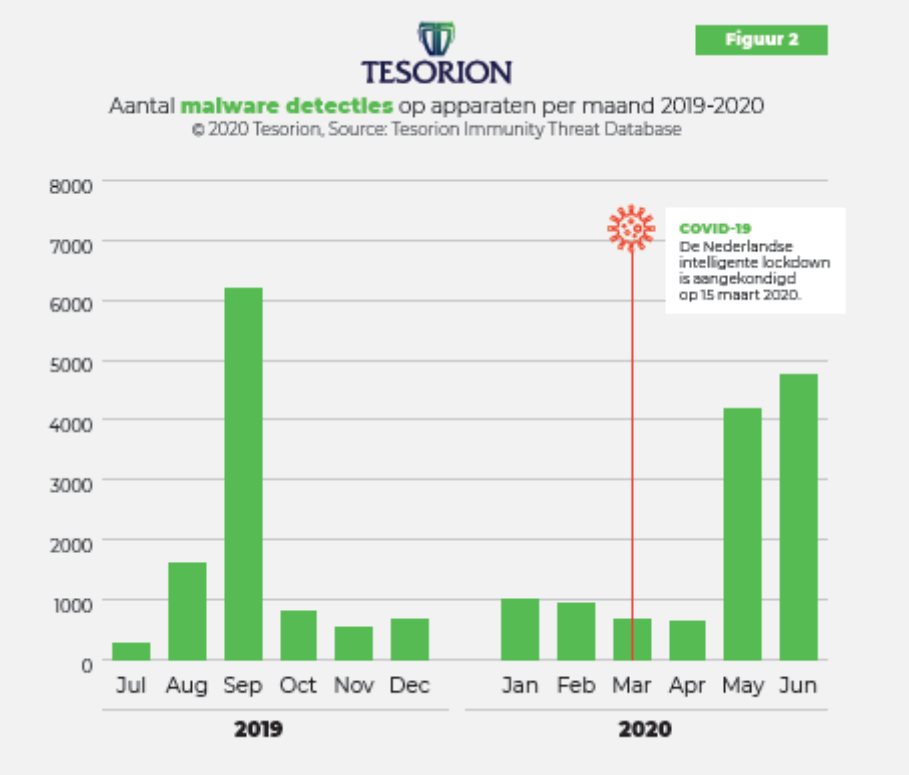
Explosief meer malware op bedrijfsnetwerken na terugkomst op de werkvloer

Leusden – Tijdens de intelligente lockdown daalde het aantal malwaremeldingen op bedrijfsnetwerken behoorlijk, waarna het bij terugkeer op de werkvloer explosief steeg. Cybersecurity organisatie Tesorion zag in maart van dit jaar het aantal malware detecties op de vier miljoen apparaten van haar klanten dalen naar zo'n 600 per maand. In mei volgde een explosieve stijging en ging het aantal malware-incidenten gedetecteerd door Tesorion Immunity al over de 4.000 grens. In juni liep het zelfs tegen de 5.000 incidenten aan, wat maar liefst acht keer meer detecties waren dan in maart. Apparaten die voor thuiswerken zijn gebruikt, blijken dus veel malware te hebben opgelopen in de eerste weken van de COVID-19 crisis en namen dit vervolgens mee naar het bedrijfsnetwerk.



Meer WLAN-apparaten op netwerk is meer malware-incidenten
De pieken in malware-incidenten vallen doorgaans samen met de toenames van het aantal WLAN-apparaten op een netwerk. In mei en juni dit jaar gingen veel werknemers weer terug naar kantoor en kon malware via hun apparaat het bedrijfsnetwerk binnendringen. Op bedrijfsnetwerken, bewaakt door Tesorion, wordt malware snel gedetecteerd, maar thuis ontbreekt het regelmatig aan de juiste

securitymaatregelen. Besmette gebruikers worden hierdoor pas opgemerkt bij terugkeer in het bedrijfsnetwerk. Er was ook een piek te zien in september 2019, wat verklaard kan worden door het aantal terugkerende scholieren en studenten na de zomervakantie.

Ernst Veen, product manager bij Tesorion: “In veel bedrijfsnetwerken hebben apparaten toegang tot alle omringende apparaten. Dit geeft hackers en malware alle vrijheid en gelegenheid om andere apparaten te detecteren en besmetten. Zo kan één apparaat dat tijdens het praktisch onbeschermd thuiswerken besmet is geraakt, de gehele organisatie platleggen wanneer het weer in het bedrijfsnetwerk komt. Een eerste stap in de beveiliging van een netwerk is dan ook om het netwerk te segmenteren. Dat zorgt er voor dat eventuele dreigingen veel minder schade aanrichten. Daarnaast hebben veel phishing-acties ingespeeld op de onzekere tijd waarin we ons verkeren. Het aantal phishing-acties is toegenomen, wat uiteindelijk bijdraagt aan het piekaantal malware-incidenten. Voor de komende thuiswerkperiode is het dus ook van groot belang dat de awareness van de medewerkers wordt verhoogd als het om phishing gaat.”

Meer weten over hoe COVID-19 hackers vrij spel geeft op bedrijfsnetwerken en wat je ertegen kunt doen? 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/