Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

stop malware

Overzicht

Waarschijnlijk heeft u weleens gehoord van termen als virus, Trojan, ransomware of rootkit wanneer men spreekt over cyberveiligheid. Dit zijn verschillende soorten kwaadaardige programma's, genaamd malware, die cybercriminelen gebruiken om computers en apparaten te infecteren. Eenmaal geïnstalleerd, kunnen ze doen wat ze willen. Leer wat malware is, welk gevaar het vormt en vooral wat u kunt doen om uzelf ertegen te beschermen.

Wat Is Malware?

Simpel gezegd, is malware software - een computerprogramma - dat wordt gebruikt om kwaadaardige acties uit te voeren. Deze term is een combinatie van de woorden kwaadaardig en software. Cybercriminelen installeren malware op uw computers of apparaten om er controle over te krijgen. Eenmaal geïnstalleerd kan malware criminelen in staat stellen uw online activiteiten te bespioneren, uw wachtwoorden of bestanden te stelen of uw systeem te gebruiken om anderen aan te vallen. Malware kan zelfs de controle over uw eigen bestanden overnemen en eisen dat u losgeld betaalt om ze terug te krijgen. Veel mensen geloven dat malware alleen voor Windows-computers een probleem is. Helaas kan malware elk apparaat infecteren, van Mac-computers en smartphones tot DVR's en beveiligingscamera's. Hoe meer computers en apparaten door cybercriminelen geïnfecteerd worden, des te meer geld ze kunnen verdienen. Daarom is iedereen een target, inclusief u.

Bescherm uzelf - Stop malware

U denkt misschien dat u alleen maar een beveiligingsprogramma zoals antivirussoftware hoeft te installeren en dat u dan beschermd bent tegen infecties. Helaas kan anti-virus niet alle malware stoppen. Cybercriminelen ontwikkelen voortdurend nieuwe en geavanceerdere malware die detectie kan ontwijken. Op hun beurt werken antivirusverkopers hun producten voortdurend bij met nieuwe mogelijkheden om malware te detecteren. In veel opzichten is het een wapenwedloop geworden, en de slechteriken zijn meestal een stap voor. Aangezien u niet alleen op anti-virus kunt vertrouwen, zijn hier extra stappen die u moet nemen om uzelf te beschermen:

Cybercriminelen infecteren vaak computers of apparaten door kwetsbaarheden in uw software te misbruiken. Hoe actueler uw software, hoe minder kwetsbaarheden uw systemen hebben en hoe moeilijker het is voor cybercriminelen om ze te besmetten. Zorg ervoor dat uw besturingssystemen, toepassingen, browser- en browserplug-ins en apparaten altijd worden bijgewerkt en actueel zijn. De eenvoudigste manier om dit te garanderen is het zoveel mogelijk automatisch bijwerken.

Een veelgebruikte manier waarop cybercriminelen computers of mobiele apparaten infecteren is door valse computerprogramma's of mobiele apps te maken, deze op het internet te plaatsen en u vervolgens te misleiden om er een te downloaden en te installeren. Download en installeer alleen programma's of apps van vertrouwde online winkels. Blijf ook uit de buurt van mobiele apps die gloednieuw zijn, weinig positieve recensies hebben, zelden worden bijgewerkt of zijn gedownload door een klein aantal mensen. Gebruikt u het computerprogramma of mobiele app niet meer? Wissen.

Cybercriminelen zetten mensen er vaak toe aan om malware voor hen te installeren. Ze kunnen u bijvoorbeeld een e-mail sturen die er legitiem uitziet en een bijlage of link bevat. Misschien lijkt de e-mail van uw bank of van een vriend te komen. Als u echter het bijgevoegde bestand zou openen of op de link zou klikken, zou u kwaadaardige code activeren die malware op uw systeem installeert. Als een boodschap een sterk gevoel van urgentie creëert, of te mooi lijkt om waar te zijn, kan het een aanval zijn. Wees verdacht, gezond verstand is vaak uw beste verdediging.

Maak regelmatig een back-up van uw systeem en bestanden op cloudservices of sla uw back-ups offline op, bijvoorbeeld op losgekoppelde externe schijven. Dit beschermt uw back-ups voor het geval malware probeert ze te coderen of te wissen. Back-ups zijn van cruciaal belang, het is vaak de enige manier waarop u kunt herstellen van een malware-infectie.

De beste manier om u te verdedigen tegen malware is uiteindelijk al uw software en apparaten up-to-date te houden, waar mogelijk vertrouwde antivirussoftware te installeren en alert te zijn op iedereen die u probeert te verleiden uw eigen systeem te infecteren. Wanneer al het andere faalt, zijn regelmatige back-ups vaak de enige manier waarop u kunt herstellen.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Lenny Zeltser *bestrijdt malware door endpointbeveiligingsproducten te maken in Minerva Labs en les te geven aan het SANS-instituut. Lenny is actief op Twitter als* @lennyzeltser en schrijft een beveiligingsblog op zeltser.com.

Bronnen

Ransomware:	https://www.sans.org/u/EdI
Backups:	https://www.sans.org/u/EdN
Stop That Phish:	https://www.sans.org/u/EdS