PERSBERICHT

Kaspersky Lab ontdekt opnieuw zwakheid in Microsoft software

Utrecht, 14 november 2018 – Het is de tweede keer in afgelopen maand dat zogeheten Automatic Exploit Prevention technologie van Kaspersky Lab een nieuwe zero-day exploit ontdekt in Microsoft Windows. Deze kwetsbaarheid in de software heeft het cybersecuritybedrijf gemeld bij Microsoft waarna zij direct een beveiligingspatch hebben aangebracht.

Aanvallen via een zero-day kwetsbaarheid maken misbruik van een nog niet ontdekte – en dus ook nog niet gerepareerde – kwetsbaarheid in de software, waardoor ze moeilijk te detecteren en te voorkomen zijn. Als criminelen een dergelijke zwakke plek ontdekken, kan dat worden gebruikt voor het maken van een exploit, een speciaal kwaadaardig programma dat toegang geeft tot een volledig systeem. Dit aanvalsscenario wordt veel gebruikt bij 'advanced persistent threat' (APT) aanvallen, waarbij indringers voor langere tijd ongemerkt toegang krijgen tot een systeem.

De door Kaspersky Lab uitgevoerde analyse van de nieuwe exploit heeft de experts naar een tot dusverre onbekend zero-day-lek geleid. Hoewel de bezorgmethode nog niet bekend is, staat vast dat de exploit is uitgevoerd in de eerste fase van een malware-installatieprogramma om benodigde rechten voor het systeem te verkrijgen. Alleen de 32-bits versie van Windows 7 is ontvankelijk voor de exploit.

Het is volgens Kaspersky Lab niet duidelijk wie er achter de aanvallen zit, maar minstens één APT-actor heeft de ontwikkelde exploit gebruikt.

Begin oktober had Kaspersky Lab ook al een exploit van een zero-day-lek ontdekt in de Microsoft Windows software. Deze exploit werd bezorgd via een PowerShell-backdoor. Ook die dreiging is direct gemeld bij Microsoft.

"Zero-day-lekken komen dit najaar helaas vaker op ons vizier", zegt Jornt van der Wiel, beveiligingsdeskundige bij Kaspersky Lab. "Binnen een maand tijd hebben we er twee ontdekt, én twee aanvalsreeksen in dezelfde regio. De onopvallende modus operandi van cyberdreigingsactoren maakt dat het voor bedrijven van cruciaal belang is dat ze over tools en oplossingen beschikken die slim genoeg zijn om hen te beschermen tegen zulke geavanceerde aanvallen. Zonder de juiste hulpmiddelen, worden ze het slachtoffer van complexe aanvallen die uit het niets lijken te komen."

Om zero-day exploits te voorkomen, adviseert Kaspersky Lab de volgende maatregelen:

- Indien mogelijk, vermijd software die als kwetsbaar bekend staat of in het recente verleden met cyberaanvallen in verband is gebracht;

- Zorg ervoor, dat software wordt gebruikt die regelmatig wordt bijgewerkt naar de meest recente versie. Beveiligingsproducten met kwetsbaarheidsbeoordeling en patchbeheer kunnen helpen met de automatisering van deze processen;
- Gebruik een robuuste beveiligingsoplossing die is uitgerust met geavanceerde detectiemogelijkheden voor effectieve bescherming tegen bekende en onbekende dreigingen, waaronder exploits;
- Maak gebruik van uw bedrijf het doelwit van gerichte aanvallen zou kunnen worden, gebruik dan geavanceerde beveiligingstools als Kaspersky Anti Targeted Attack Platform (KATA) als er sprake is van gerichte cyberaanvallen;
- Zorg dat de meest recente beveiligingsinformatie toegankelijk is voor relevante betrokkenen.

Meer informatie is te vinden op Securelist.com.

WEBSITE | **CORPORATE NIEUWS** | **PRODUCT & DIENSTEN** | **NEWSROOM**

Over Kaspersky Lab

Kaspersky Lab is een wereldwijd opererend cybersecuritybedrijf dat langer dan 20 jaar actief is op de markt. Kaspersky Labs beveiligingsoplossingen en -diensten ter bescherming van bedrijven, kritieke infrastructuur, overheden en consumenten zijn gebaseerd op diepgaande kennis en ervaring. Het uitgebreide beveiligingsportfolio van het bedrijf omvat toonaangevende endpoint-bescherming en gespecialiseerde beveiligingsoplossingen en diensten voor de bestrijding van geavanceerde en voortdurende veranderende digitale dreigingen. Technologieën van Kaspersky Lab bieden bescherming aan ruim 400 miljoen gebruikers en helpen 270.000 zakelijke klanten om hun meest waardevolle bezit te beschermen. Meer informatie op www.kaspersky.com.

Noot voor redacties:

Voor meer informatie kunt u contact opnemen met onderstaande contactpersonen. Indien u niet langer persberichten wenst te ontvangen, stuurt u dan een e-mail aan info@communicationforce.com.

Contactgegevens:	**Kaspersky Lab**	**The Communication Force**
	Caroline Breure	Jan Poté
	Tel. +31 (0)30 – 752 95 00	Tél. +32 (0) 475 925 582
	caroline.breure@kaspersky.nl	jan.pote@gmail.com