Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 24 november 2023

Toegestane verspreiding: TLP:GREEN
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:GREEN en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Welkom bij de End of Week van vrijdag 24 november 2023.

Het is vandaag Black Friday, wat betekent dat honderden winkels en webwinkels stunten met allerlei aanbiedingen. Niet geslaagd! dan kunt u wellicht nog aankomende maandag een deal scoren tijdens Cyber Monday. Maar let wel op: valse reclame pop-ups, spam en webshops te over!

In deze End of Week vertel ik graag iets over DarkGate en PikaBot Malware, een relatief nieuwe ransomware actor, kwetsbaarheden in Windows Hello en tot slot een blogpost van Citrix met aanvullend handelingsperspectief.

DarkGate en PikaBot Malware

In het steeds veranderende landschap van cyberdreigingen is een geavanceerde phishing-campagne opgedoken waarmee Darkgate-malware is verspreid. Daarnaast neemt het gebruik van PikaBot, een andere initial access malware, ook toe en vertonen beide campagnes (DarkGate en PikaBot) een vergelijkbaar infectiepatroon. De recente stilte rond QakBot nadat infrastructuur was neergehaald door een internationale actie van politie- en justitiediensten in augustus, is ook weer verbroken nadat er recentelijk nieuwe malware ontdekt is die dezelfde overeenkomsten vertoont als QakBot [1]

INC Ransom

Cybereason heeft in een blogpost geschreven over een dreiging van een relatief nieuw ransomware-actor genaamd "INC Ransom". INC Ransom lijkt zich te richten op de Verenigde Staten en Europese landen. De slachtoffers zijn voornamelijk bedrijven uit de commerciële sector, al is ook tenminste één overheidsorganisatie slachtoffer geworden van de actor. Als het om de modus operandi gaat, zijn de INC-gevallen volgens Cybereason vergelijkbaar met die van andere ransomware groepen. De actor maakt gebruikt van gecompromitteerde inloggegevens om toegang tot systemen te krijgen waarbij ze met behulp van RDP (Remote Desktop Protocol) zich verder lateraal verplaatsen. Volgens Cybereason maakt INC Ransom bij data exfiltraties gebruik van de tool MegaSync. [2]

Windows Hello

Een nieuw onderzoek heeft meerdere kwetsbaarheden aan het licht gebracht die kunnen worden misbruikt om "Windows Hello" [3] authenticatie op Dell Inspiron 15,

[1] https://thehackernews.com/2023/11/darkgate-and-pikabot-malware-resurrect.html

[2] https://www.cybereason.com/blog/threat-alert-inc-ransomware

[3] https://support.microsoft.com/en-us/windows/learn-about-windows-hello-and-set-it-up-dae28983-8242-bb2a-d3d1-87c9d265a5f0

Lenovo ThinkPad T14 en Microsoft Surface Pro X-laptops te omzeilen. De kwetsbaarheden werden ontdekt door onderzoekers van Blackwing Intelligence, die de kwetsbaarheden ontdekten in de vingerafdruksensoren van Goodix, Synaptics en ELAN die in de apparaten zijn ingebed. Eén voorwaarde voor misbruik van de vingerafdruklezer is dat de gebruikers van de beoogde laptops al vingerafdruk authenticatie hebben ingesteld. [4]

Citrix Netscaler

Afgelopen maandag heeft Citrix aanvullend handelingsperspectief gepubliceerd in een blogpost over een kwetsbaarheid in Netscaler ADC en Netscaler Gateway. Deze kwetsbaarheid wordt ook wel "CitrixBleed" genoemd. In de blogpost geeft Citrix aan dat na het installeren van de updates, actieve of blijvende gebruikerssessies verwijderd moeten worden. Kwaadwilenden hebben gebruikerssessies buit-gemaakt bij voorheen kwetsbare Citrix servers. Deze gebruikerssessies kunnen mogelijk nog misbruikt worden nadat updates geïnstalleerd zijn en alsnog tot compromittatie van het netwerk leiden als de bestaande sessies niet zijn verwijderd. [5] [6]

[4] https://thehackernews.com/2023/11/new-flaws-in-fingerprint-sensors-let.html

[5] https://www.netscaler.com/blog/news/netscaler-investigation-recommendations-for-cve-2023-4966/

[6] https://www.ncsc.nl/actueel/advisory?id=NCSC-2023-0517

Beveiligingsadviezen

Zie voor een actueel overzicht: www.ncsc.nl/actueel/beveiligingsadviezen

NCSC-2023-0517 [v1.04] [H/H]	Kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway
NCSC-2023-0611 [v1.00] [M/H]	Kwetsbaarheden verholpen in Nagios XI
NCSC-2023-0612 [v1.00] [M/H]	Kwetsbaarheid verholpen in Splunk
NCSC-2023-0613 [v1.00] [M/H]	Kwetsbaarheden ontdekt in OwnCloud
NCSC-2023-0614 [v1.00] [M/H]	Kwetsbaarheden verholpen in Atlassia producten
NCSC-2023-0615 [v1.00] [M/M]	Kwetsbaarheden verholpen in Mozilla Firefox en Thunderbird
NCSC-2023-0616 [v1.00] [M/H]	Kwetsbaarheden verholpen in Foxit PDF Reader en PDF Editor

Wat was er nog meer in het nieuws

Bug bounty programma

Microsoft heeft een nieuw bugbounty-programma gelanceerd, dit keer met als doel zijn producten en diensten van het merk Microsoft Defender veerkrachtiger te maken tegen aanvallen. Het Microsoft Defender Bounty Program biedt ethische hackers tussen de $500 en $20.000 voor significante kwetsbaarheden die een directe en aantoonbare impact hebben. Het grootste bedrag voor een nieuwe kwetsbaarheid gaat naar onderzoekers die kritieke bugs in de uitvoering van Remote Code Execution kunnen vinden. Kwetsbaarheden die binnen de reikwijdte vallen, zijn onder meer cross-site scripting, Cross site request forgery (CSRF), Server side request forgery (SSRF), Cross-tenant data tampering or access en Injection vulnerabilities. [7]

The Dragon Touch KidzPad Y88X

Een onderzoeker bij Electronic Frontier Foundation heeft sporen van Corejava malware gevonden in de Dragon Touch KidzPad Y88X. Niet alleen is er malware gevonden, de tablet draait een versie van Android die vijf jaar geleden werd uitgebracht. De tablet werd geleverd met een vooraf geïnstalleerde en verouderde versie van de KIDOZ-app, die dienstdoet als app store waarmee ouders ouderlijk toezicht kunnen instellen en kinderen games en apps kunnen downloaden. Volgens de onderzoeker verzamelt en verzendt de app store gegevens naar "kidoz.net" over het gebruik en de fysieke kenmerken van het apparaat zoals apparaat model, merk, land, tijdzone, schermgrootte, weergavegebeurtenissen, klikgebeurtenissen, logtijd van gebeurtenissen en een unieke KID-ID. [8]

Huntress

Huntress heeft een dreigingsrapport gepubliceerd voor het MKB. Het rapport levert waardevolle inzichten over opkomende cyberdreigingen die zich richten op het MKB, en biedt kennis over hoe bedrijven zich hiertegen kunnen verdedigen. Na het invoeren van een e-mail adres en bedrijfsnaam is het rapport gratis te downloaden.[9]

Indicators of Compromise

Het Britse National Cyber Security Centre heeft een nieuwe RFC over Indicators of Compromise gepubliceerd om cyberbeveiliging bij het ontwerpen van protocollen te ondersteunen. NCSC-UK hoopt hiermee meer cyberverdedigers aan te moedigen zich met internationale normen bezig te houden. RFC's zijn referentiedocumenten met technische specificaties en organisatorische aantekeningen voor de technische grondslagen van het internet. [10]

[7] https://msrc.microsoft.com/blog/2023/11/introducing-the-microsoft-defender-bounty-program/

[8] https://www.hackread.com/dragon-touch-tablets-kids-corejava-malware/

[9] https://www.huntress.com/resources/report/smb-threat-report

[10] https://www.ncsc.gov.uk/blog-post/rfc-indicators-of-compromise-for-ietf

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

november ’23

TLP:GREEN