GEZAMENLIJKE VERKLARING VAN HET FEDERAL BUREAU OF INVESTIGATION (FBI), DE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), HET OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI) EN DE NATIONAL SECURITY AGENCY (NSA)

Oorspronkelijke releasedatum: 5 januari 2021

Namens president Trump heeft het personeel van de National Security Council een taskforce-constructie opgericht die bekend staat als de Cyber Unified Coordination Group (UCG), bestaande uit de FBI, CISA en ODNI met steun van de NSA, om het onderzoek en de sanering van dit belangrijke cyberincident waarbij federale overheidsnetwerken betrokken waren. Het UCG werkt nog steeds aan de reikwijdte van het incident, maar heeft de volgende updates over zijn onderzoeks- en mitigatie-inspanningen.

Dit werk geeft aan dat een Advanced Persistent Threat (APT) -acteur, waarschijnlijk van Russische oorsprong, verantwoordelijk is voor de meeste of alle recent ontdekte, voortdurende cybercompromissen van zowel overheids- als niet-gouvernementele netwerken. Op dit moment denken we dat dit een inspanning was en blijft om inlichtingen te verzamelen. We nemen alle nodige stappen om de volledige reikwijdte van deze campagne te begrijpen en dienovereenkomstig te reageren.

De UCG is van mening dat van de ongeveer 18.000 getroffen klanten in de publieke en private sector van het Orion-product van Solar Winds, een veel kleiner aantal in gevaar is gebracht door vervolgactiviteiten op hun systemen. We hebben tot dusver minder dan tien Amerikaanse overheidsinstanties geïdentificeerd die in deze categorie vallen, en werken eraan om de niet-gouvernementele entiteiten te identificeren en op de hoogte te stellen die mogelijk ook worden beïnvloed.

Dit is een serieus compromis dat een aanhoudende en toegewijde inspanning vereist om te herstellen. Sinds de eerste ontdekking heeft het UCG, met inbegrip van hardwerkende professionals uit de hele Amerikaanse regering, en onze partners uit de particuliere sector non-stop gewerkt. Deze inspanningen hielden niet op tijdens de vakantie. Het UCG zal alle noodzakelijke maatregelen blijven nemen om onderzoek te doen, te corrigeren en informatie te delen met onze partners en het Amerikaanse volk.

Als leidende instantie voor reactie op dreigingen, is het onderzoek van de FBI momenteel gericht op vier cruciale inspanningen: het identificeren van slachtoffers, het verzamelen van bewijsmateriaal, het analyseren van het bewijs om verdere toeschrijving te bepalen, en het delen van resultaten met onze overheid en partners uit de particuliere sector om operaties, inlichtingenbeeld en netwerkverdediging.

CISA is de hoofdrolspeler voor asset response en richt zich op het snel delen van informatie met onze overheidspartners en partners uit de particuliere sector, terwijl we proberen de omvang van deze campagne en het exploitatieniveau te begrijpen. CISA heeft ook een gratis tool ontwikkeld voor het detecteren van ongebruikelijke en mogelijk schadelijke activiteiten met betrekking tot dit incident. In een noodrichtlijn die op 14 december werd gepost, regisseerde CISA de snelle ontkoppeling of uitschakeling van getroffen SolarWinds Orion-producten van federale netwerken. CISA heeft ook een technische waarschuwing afgegeven met technische details en risicobeperkende strategieën om netwerkverdedigers te helpen onmiddellijk actie te ondernemen. CISA zal alle bekende details blijven delen zodra deze beschikbaar komen.

Als hoofd voor inlichtingenondersteuning en aanverwante activiteiten coördineert ODNI de inlichtingengemeenschap om ervoor te zorgen dat het UCG beschikt over de meest up-to-date informatie om de mitigatie- en responsactiviteiten van de Amerikaanse regering te sturen. Verder biedt ODNI, als onderdeel van zijn missie voor het delen van informatie, situationeel bewustzijn aan de belangrijkste belanghebbenden en coördineert het activiteiten voor het verzamelen van inlichtingen om kennislacunes aan te pakken.

Ten slotte ondersteunt de NSA het UCG door informatie, cybersecurity-expertise en bruikbare begeleiding te bieden aan de UCG-partners, evenals aan de eigenaren van National Security Systems, het ministerie van Defensie en de eigenaars van het industriële basissysteem van Defensie. Het engagement van NSA met zowel het UCG als de industriële partners is gericht op het beoordelen van de schaal en de omvang van het incident, en op het bieden van technische risicobeperkende maatregelen.

Het UCG blijft erop gericht ervoor te zorgen dat slachtoffers worden geïdentificeerd en hun systemen kunnen herstellen, en dat bewijsmateriaal wordt bewaard en verzameld. Aanvullende informatie, inclusief indicatoren van compromissen, zal openbaar worden gemaakt zodra deze beschikbaar komt.

Zie voor aanvullende bronnen:

- CISA-tool voor het detecteren van verdachte activiteiten: https://github.com/cisagov/Sparrow
- 12/22 FBI-kennisgeving particuliere sector

- CISA Insights: wat elke leider moet weten over de lopende APT-cyberactiviteit
- CISA Alert: Advanced Persistent Threat Compromise van overheidsinstanties, kritieke infrastructuur en particuliere organisaties
- NSA Cybersecurity-advies: kwaadwillende actoren misbruiken authenticatiemechanismen om toegang te krijgen tot cloudbronnen
- December 16, 2020 Joint UCG Statement

###

Onderwerpen
Cybersecurity
Sleutelwoorden
Cybersecurity
Laatste publicatiedatum: 5 januari 2021