Declarație comună a Biroului Federal de Investigații (FBI), Agenția pentru Securitatea Cibernetică și Securitatea Infrastructurii (CISA), Office of the Director of National Intelligence (ODNI), și Agenția pentru Securitatea Națională (NSA)

În numele Președintelui Trump, personalul Consiliului Securității Naționale al Statelor Unite ale Americii a organizat un task force cunoscut sub denumirea **Grupul de Coordonare Cyber Unit** (UCG), compus din FBI, CISA și ODNI, cu sprijinul NSA, pentru a coordona investigarea și remedierea unui incident cibernetic semnificativ care implică rețelele federale guvernamentale. UCG încă lucrează pentru a înțelege scopul incidentului, dar are câteva informații actualizate cu privire la eforturile sale de investigare și remediere.

Acest proces arată că un actor Advanced Persistent Threat (APT), probabil de origine rusă, este responsabil pentru majoritatea, sau chiar toate compromiterile cibernetice recente ale rețelelor guvernamentale și non-guvernametale. În acest moment, credem că a fost, și continuă să fie, un efort de colectare a unor informații corespondente activității de intelligence. Facem toți pașii necesari pentru a înțelege întregul scop al campaniei și pentru a răspunde corespunzător.

UCG consideră că, dintre cei aproximativ 18.000 de clienți publici și privați afectați de produsul Solar Winds Orion, un număr mult mai mic au fost compromiși prin activități ulterioare desfășurate pe sistemele lor. Am identificat până acum mai puțin de 10 agenții guvernamentale americane ce intră în această categorie și lucrăm la identificarea și notificarea entităților non-guvernamentale care au fost afectate.

Aceasta este o compromitere serioasă ce va necesita un efort dedicat și susținut pentru remediere. Încă de la momentul descoperirii inițiale, UCG, alături de profesioniști din cadrul Guvernului Statelor Unite, precum și partenerii noștri din sectorul privat, au lucrat non-stop. Aceste eforturi nu au fost oprite de sărbători. UCG va continua să facă fiecare acțiune necesară pentru a investiga, remedia și împărtăși informațiile cu partenerii noștri și cu poporul american.

Ca agenție cu rol de lider în răspunsul la amenințări, FBI își concentrează investigația pe 4 linii critice de efort: identificarea victimelor, strângerea dovezilor, analizarea dovezilor pentru determinarea atribuirii viitoare și împărtășirea rezultatelor cu partenerii din sectorul guvernamental și privat.

Ca lider în ceea ce privește activele existente, CISA este concentrată pe diseminarea rapidă de informații cu partenerii din sectorul guvernamental și privat, în cadrul eforturilor de înțelegere a extinderii campaniei și a nivelului de exploatare. CISA a creat și un instrument gratis pentru detectarea activităților neobișnuite sau potential periculoase legate de acest incident.

Într-o Directivă de Urgență publicată pe 14 decembrie, CISA a dirijat deconectarea rapidă sau oprirea produselor afectate SolarWinds Orion din rețelele federale. CISA a emis și o alertă tehnică furnizând detaliile tehnice și strategiile de remediere pentru a ajuta administratorii de rețea să adopte acțiuni imediate. CISA va continua să împărtășească orice detalii cunoscute de îndată ce vor fi disponibile.

Ca lider pentru suport de tip intelligence și activități aferente, ODNI coordonează comunitatea de intelligence și se asigură că UCG deține informații actualizate pentru a realiza activități de ameliorare și de răspuns la aceast tip de amenințare pentru Guvernul Statelor Unite. În plus, ca parte a misiunii de diseminare a informațiilor, ODNI furnizează informații de conștinentizare și coordonează activitățile de strângere a informațiilor de intelligence.

Nu în ultimul rând, NSA sprijină UCG prin furnizarea de intelligence, expertiză în domeniul securității cibernetice și îndrumare a partenerilor UCG, precum și pentru propietarii de sisteme din cadrul Sistemelor de Securitate Națională, Departamentul Apărării și industria de apărare.

Colaborarea NSA cu UCG și partenerii de industrie este concentrată pe stabilirea nivelului de impact și obiectivului incidentului, precum și pe furnizarea de măsuri de remediere tehnică.

UCG rămâne concentrat pe asigurarea faptului că toate victimele sunt identfiicate și pot remedia sistemele, dar și că dovezile sunt protejate și strânse corespunzător. Informații adiționale, referitoare la indicatori de compromis, vor fi făcute publice în momentul în care vor fi disponibile.

Pentru resurse suplimentare vă rugăm să accesați:

- 12/22 FBI Private Industry Notification
- CISA Insights: What Every Leader Needs to Know About the Ongoing APT Cyber Activity
- CISA Alert: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- NSA Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources
- December 16, 2020 Joint UCG Statement

Materialul este o traducere în limba română a **Declarației comune** publicată pe site-ul cisa.gov.

Sursa originală: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure