CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE
DE SECURITATE CIBERNETICĂ – CERT-RO

LISTĂ DE RESURSE ÎN CONTEXTUL ATACULUI CIBERNETIC DE TIP SUPPLY CHAIN VIA SOLARWINDS ORION

Versiune 21.12.2020

În ultimele zile, comunitatea de cybersecurity a fost alertată în privința unui **atac cibernetic de tip supply chain** prin actualizările furnizate de compania **SolarWinds** pentru **SolarWinds Orion**.

VEZI MAI MULTE DETALII AICI

Acesta este unul dintre cele mai periculoase scenarii pentru multe organizații: un actor avansat sponsorizat de un stat poate să fi avut deja acces la infrastructurile organizației dumneavoastră timp de mai multe luni, printr-un backdoor nedetectat.

Drept urmare, specialiști în domeniu au început documentarea problemei, iar unul dintre pașii pentru remediere implică acțiuni strict necesare pentru a izola, eradica și remedia backdoorul de la SolarWinds. Având în vedere pericolul generat de un astfel de atac pentru infrastructuri informatice, echipa CERT-RO vă pune la dispoziție o listă de resurse publice utile:

Data publicării	Sursa / Titlu / Detalii	Link către sursa informației
2020.12.08	FireEye - Threat Research - Unauthorized Access of FireEye Red Team Tools	https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html
2020.12.13	FireEye - Threat Research - Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor	https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
2020.12.16	RedDrip7 - SunBurst_DGA_Decode	https://github.com/RedDrip7/SunBurst_DGA_Decode
2020.12.17	TrustedSec - Solarwinds backdoor (Sunburst) incident response playbook	https://www.trustedsec.com/blog/solarwinds-backdoor-sunburst-incident-response-playbook/
2020.12.17	Alex Eckelberry- Preliminary list (with disclaimers) into who was hacked in the Sunburst attack	http://blog.eckelberry.com/a-preliminary-look-into-who-was-hacked-in-the-sunburst-attack/
2020.12.17	Security Lab - SolarWinds SUNBURST backdoor assessment	https://www.hornetsecurity.com/en/threat-research/solarwinds-sunburst-backdoor-assessment/

Data publicării	Sursa / Titlu / Detalii	Link către sursa informației
2020.12.17	Palo Alto - Threat Brief: SolarStorm and SUNBURST Customer Coverage	https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/
2020.12.18	FireEye - Indicators of Compromise (IoCs)	https://github.com/fireeye/sunburst_countermeasures
2020.12.18	Sunburst DGA 2 Domain List.txt	https://intelx.io/?s=68ef7949-8ebd-4cfb-98ad-7eda25f26cc5
2020.12.18	US DHS - Emergency Directive 21-01 Supplemental Guidance	https://cyber.dhs.gov/ed/21-01/#supplemental-guidance
2020.12.19	US CERT - Alert (AA20-352A)	https://us-cert.cisa.gov/ncas/alerts/aa20-352a
2020.12.19	Prevasio - Updated list (with disclaimers) into who was hacked in the Sunburst attack	https://blog.prevasio.com/2020/12/sunburst-backdoor-part-ii-dga-list-of.html
2020.12.20	SolarWinds - Security Advisory	https://www.solarwinds.com/securityadvisory

Aveți suspiciuni că organizația dumneavoastră a fost compromisă de atacul SolarWinds Orion?

alerts@cert.ro www.cert.ro Tel: 1911