CTI jelentés

A Solarwinds incidens

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat
NEMZETI KIBERVÉDELMI INTÉZET

Bevezetés

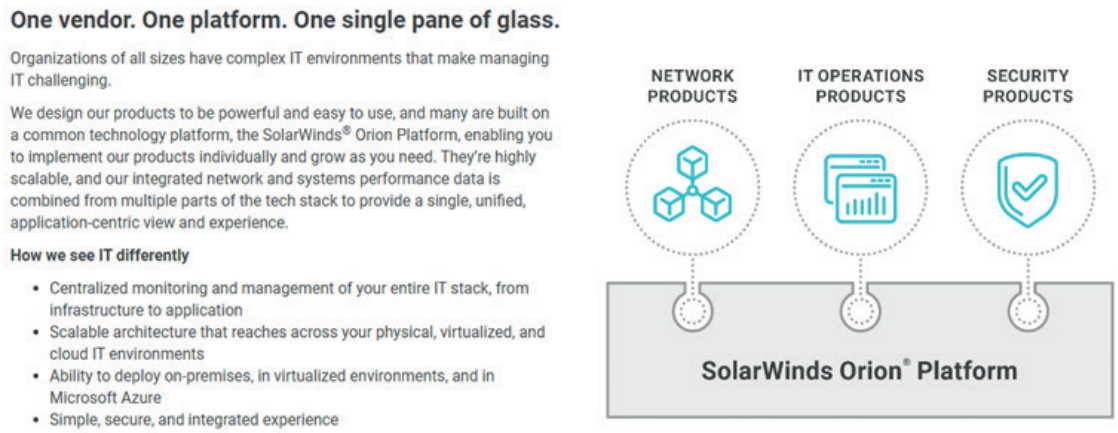
2019 végén, 2020 elején kirobbant világjárvány hatalmas változást hozott az informatika világában. A fertőzés terjedésének lassítása érdekében törekedett mindenki minimalizálni a fizikális kontaktust és így elkerülni a megfertőződést is. Az internet, amelynek legfőbb célja a kommunikáció különböző informatikai rendszerek között, megfelelő eszköz arra is, hogy kontaktus nélkül juttassunk el információkat a világ egyik feléből a másikba, a másodperc tört része alatt. Így a világon szinte minden országban **megkezdődött a teljes életünk internetre költöztetése**. Az iskolai **oktatási rendszer** interneten keresztül folytatta működését, a cégeknél bevezetésre került "**home office**" munkarend. Ezek a folyamatok hirtelen kezdőtek meg és sok cégnél nem volt megfelelően kiépítve az infrastruktúra, amely a biztonságos távoli hozzáférést biztosította volna dolgozók számára. Így a figyelem az üzemeltetési szakamberekre összpontosult, akik versenyre kelve az idővel, megpróbálták felkészíteni a meglévő rendszereket a **biztonságos távoli munkavégzésre**. Így történhetett meg, hogy amíg a szakemberek nagyban építették a biztonságot nyújtó "falakat", addig a támadók kihasználták ezt a helyzetet és szabadon garázdálkodtak a kibertérben. Ennek eredményként robbant ki a **SolarWinds botrány** is.

Tartalomjegyzék

A SolarWinds-ről röviden

A SolarWinds egy 1999-ben alapított amerikai cég, amely a **hálózatok és informatikai infrastruktúrák** folyamatos menedzselésére szakosodott. A cég legsikeresebb terméke az **Orion platform**, több mint 300.000 ügyfél használja.

Az Orion-t a **teljes informatikai infrastruktúra központi menedzselésére** tervezték, rendelkezik hálózati forgalom, szerverek, valamint szolgáltatások monitorozására alkalmas modulokkal. Ezt a terméket nem csak a multi cégek használták a több ezer számítógéppel és szerverrel rendelkező infrastruktúrájuk kordábantartására, hanem amerikai állami szervezetek is. Ezek közé tartozik az amerikai Külügyminisztérium, Belbiztonsági minisztérium, Energiaügyi minisztérium, emellett a Nemzeti Nukleáris Bizottság, Kiberbiztonsági és Infrastrukturális Ügynökség, Egészségügyi Minisztérium és a Kereskedelmi Minisztérium is.



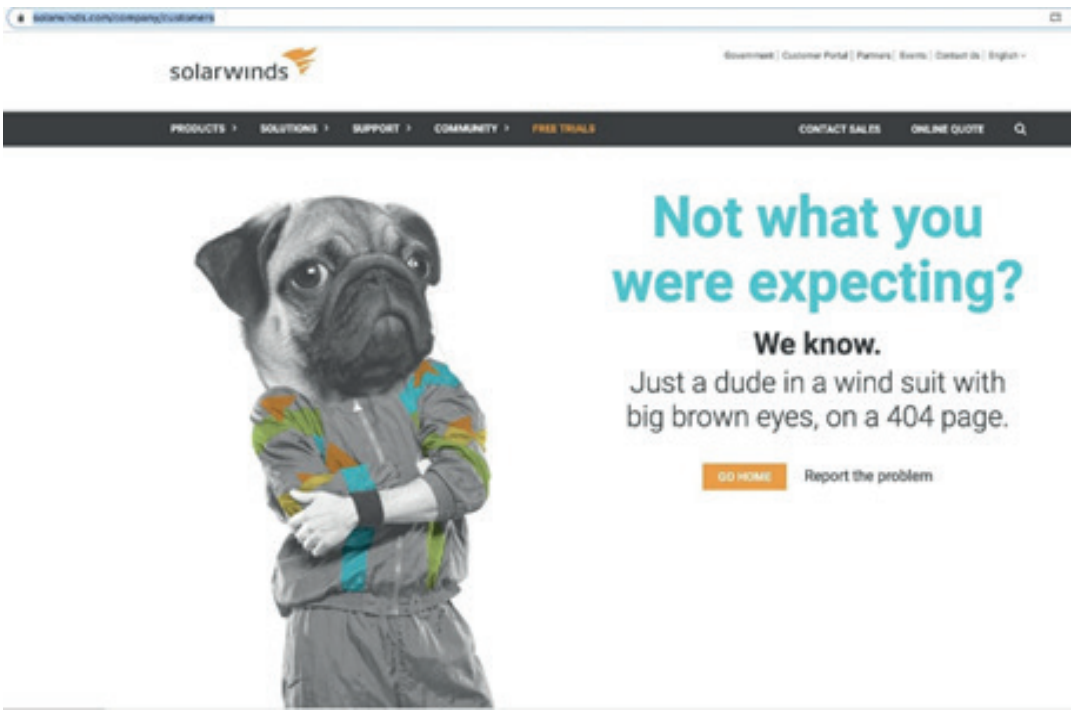
1. ábra: Az Orion platform jellemzői

Incidensek

2019-ben egy biztonsági kutató bejelentést tett a SolarWinds cégnél, hogy a frissítésért felelős szolgáltatásuk hitelesítése **gyenge jelszóval** van védve (solarwinds123), viszont ezzel nem foglalkozott a cég érdemben. 2020 márciusában az APT29 vagy CozyBear nevet viselő hacker kollektíva - akik feltehetőleg az orosz SRV-nek dolgoztak (korábban KGB-ként ismerhető) - elhelyeztek egy **hátsó kaput** (backdoor) **az Orion platform szoftver frissítései között**. Azok a felhasználók, akik március és június között letöltötték a szoftverfrissítést akaratlanul is **hozzáférést adtak** az SRV-nek a **teljes hálózatukhoz**. Ezt **supply-chain (ellátási lánc) támadásnak** nevezik, mivel a támadni kívánt szervezet egy beszállítóját - és ezáltal a beszállító összes ügyfelét is - célozzák. A támadást sokáig egyetlen szervezet sem detektálta, így a backdoor közel fél évig szabad bejárást biztosított a hacker csaport számára.

A FireEye nevű amerikai szervezet kiterjedt portfolióval rendelkezik a kiberbiztonság defenzív és offenzív oldalán is. A cégnek van egy Red Team csapata, amely az offenzív támadásokat hajtja végre. Utóbbi a bűnszervezetekbe való beépülés és azok támadását szolgálja. Ez a csapat rendelkezett egy kisebb arzenállal felérő támadó kóddal, amelyek sérülékenységek kihasználására alkalmasak, nem beszélve a 0. napi (zero day) sérülékenységek kihasználására épülő támadókódokról.

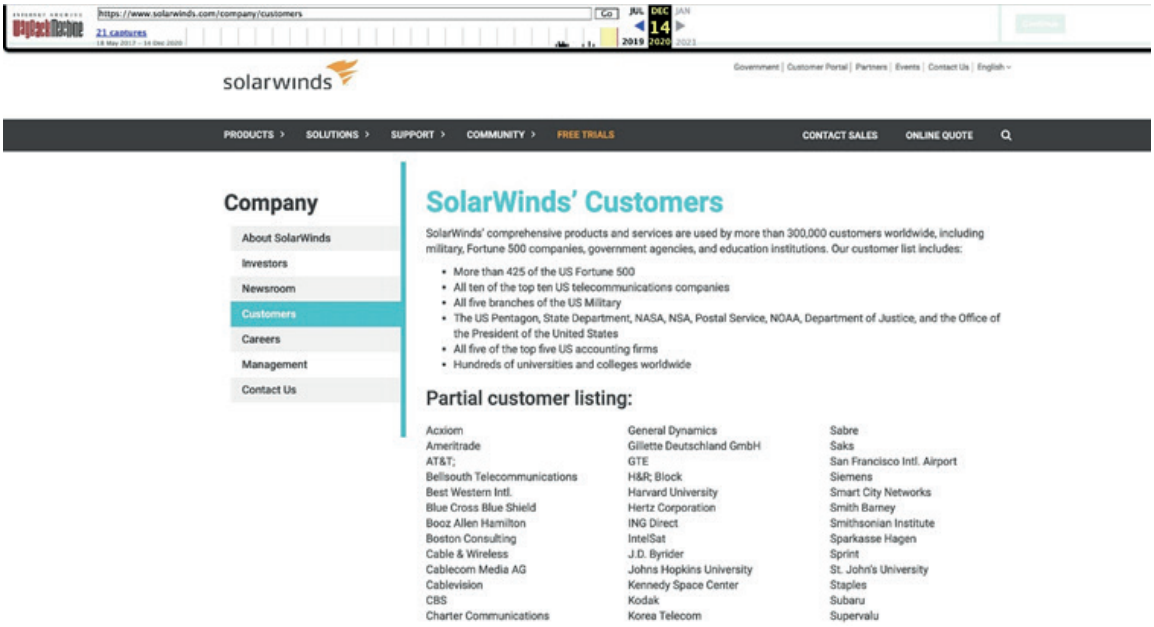
2020. december 8-án a cég bejelentette, hogy egy állami támogatású ismeretlen **hackercsoport bejutott a FireEye hálózatába** és ellopták a támadó kódjaikat. A behatolás felderítése során tapasztalták a biztonsági kutatók, hogy az **Orion platformban található backdoor segítségével juthattak be** a rendszerükbe. A Red Team kódok kiszivárgása után a FireEye kiadott az expoitok észlelésére alkalmas szabályscsomagot*, emellett a helyzet súlyosságának tekintetében felvette a kapcsolatot a rendfenntartó szervekkel is. A kódbázis kompromitációjáról való értesülés után a SolarWinds cég levette ügyfelei listáját a weboldaláról.



2. ábra: Eltávolított ügyféllista

* (https://github.com/fireeye/red_team_tool_countermeasures)

Az Internet Archive alapítvány által működtetett weboldalak tükrözésével foglalkozó szolgáltatás viszont elmentette az oldal eredeti tartalmát.



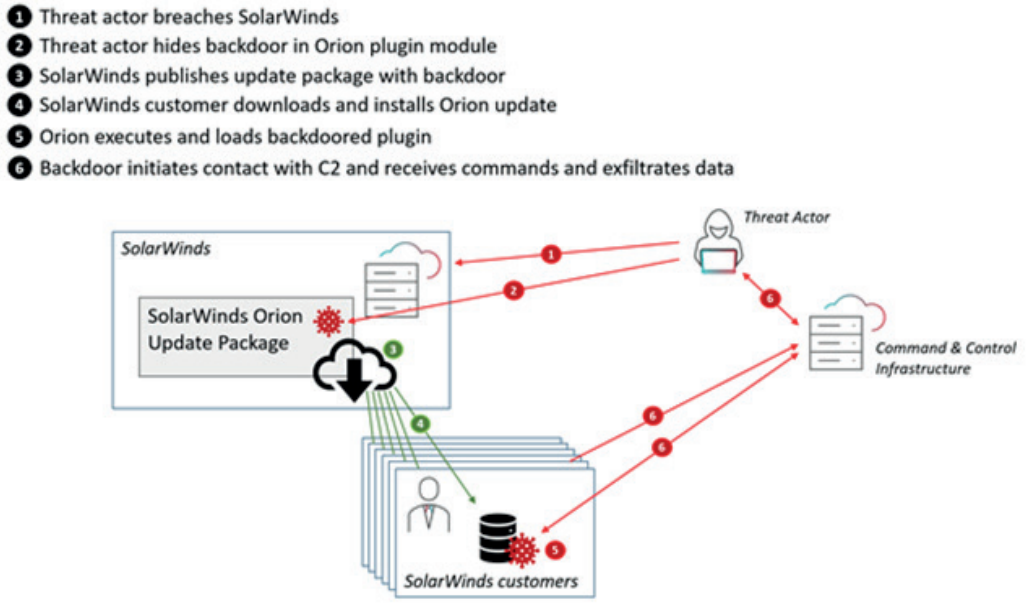
3. ábra: WayBackMachine által megőrzött tartalom

Az előbbiekben felsorolt állami szervezeteken kívül a Fortune 500-as listából **425 céget érintett kritikusan** az alábbi incidens. Decemberi bejelentésükben **18.000 ügyfelet** tartottak számon, akik **telepítették a vírusos frissítést**. A Microsoft cég statisztikai adataiból kiderül, hogy **40 cégnél** történtek **szivárogtatások**, amelyek összeköthetőek ezzel a sérülékenységgel. Bruce Schneier biztonsági kutató ezt az incidenst úgy azonosítja, hogy ez **világ szintű kémkedési tevékenység** volt, amely **nem csak Amerika ellen** irányult. A nyomozások még zajlanak, minden nap újabb információk kerülnek elő a támadással kapcsolatban.

Technikai részletek

A támadók közvetlenül nem tudtak hozzáférést szerezni az általuk megcélzott infrastruktúrákhoz, így a szoftver beszállítók között kerestek sebezhetőséget. Egy állami rendszert sokkal jobban védenek, illetve nagyobb a védelmi költségvetés is, mint egy, a privát szférában működő szoftverkészítő cégnél. Az első fázis a **felderítés** volt, amihez a SolarWinds cég ideális célpontot jelentett, mivel a monitorozó rendszerük működéséhez a teljes informatikai infrastruktúrához hozzá kell férni. A támadóknak sikerült **hozzáférést** szerezni **a cég kódtárához**, amelyet még a mai napig sem tudnak, hogy miként juthattak be az elkövetők. A második fázis a fegyverkezés. A szoftver kódját felhasználva készítettek egy **backdoor**-t, amit **sikeresen fel is töltöttek** a kódtárba. Az Orion platform 2019.4 HF verziójáról a 2020.2.1 verzióra való átállás esetén az üzemeltetők ezt a backdoort is telepítettek a rendszerükre. A harmadik fázis, a **terjesztés** a frissítés formájában valósult meg. A **kártékony kódot**, ami egy úgynevezett DLL (Dynamic Link Library), a SolarWinds.Orion.Core.BusinessLayer.dll nevű állomány tartalmazta. Az ártalmas modul a cég tanúsítványával* **digitálisan alá volt írva**. A komponens tartalmazott egy **backdoor**-t, amely egy **távoli szerverrel kommunikált**.

* (Sorozatszám: 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed)



4. ábra: A támadás menete

A FireEye cég **SUNBURST** névre keresztelte el a komponenst és kiadott egy **nyílt forrású detektáló készletet**, amely segítségével a nagyobb IPS/IDS rendszerek és vírusírtók is fel tudták ismerni a támadás jelenletét a belső hálózatokon, illetve a már települt kártevő jelenlétét a számítógépeken*. A rosszindulatú frissítés telepítése utána a kártevő elérte a negyedik fázisát, a **támadási fázist**, az életciklusa elején a backdoor **12-14 napig inaktív** állapotban marad. Ez egy bevált módszer ahhoz, hogy sikeresen átverjék az automatizált sandbox futtató környezeteket és vírusírtókat is.

A nyugalmi időszak után a program lekérdezte és **végrehajtotta a parancsokat**, amelyeket „Jobs”-nak nevezett. Ez az utasítás halmaz tartalmazta a fájlok átviteléhez, fájlok futtatásához, rendszer újraindításához, rendszer szolgáltatások inaktiválásához szükséges képességeket.

* (https://github.com/fireeye/sunburst_countermeasures)

A kártevő a hálózati **kommunikációját** az Orion Improvement Program (OIP) protokolljával **álcázta**, amely funkció a kívánt működés esetén a **gyűjtött** telemetria **adatokat** anonimizálva juttatja el a SolarWinds cégnek, így segítve a munkájukat. A gyűjtött felderítési adatokat a program a legitim szoftver konfigurációs fájljaiban tárolta el, így **elrejtve illegitim viselkedését**.

A backdoor több obfuszkált tiltó listával is rendelkezett, amellyel azonosítani tudta a nyomozati szoftvereket, vírusírtókat, amelyek a folyamatokban, szolgáltatásokban vagy hardver illesztő szoftverekben bújhattak meg. Abban az esetben, ha nem talált fenyegetésre okot adó szolgáltatást, a program az internet felől való elérhetőségét az api.solarwinds.com domain DNS címének feloldásával ellenőrizte. A trójai ezután a „avsvmcloud.com" domain az ad-hoc generált subdomain értékével **próbálta felvenni a kapcsolatot**, amely DNS válasz formájában visszaadta a C2C (Command and Control) szerver IP címét. Emellett az úgynevezett „A" rekord IP értéke **szabályozta a kártevő működését**, az előre belekódolt végrehajtási lista alapján.

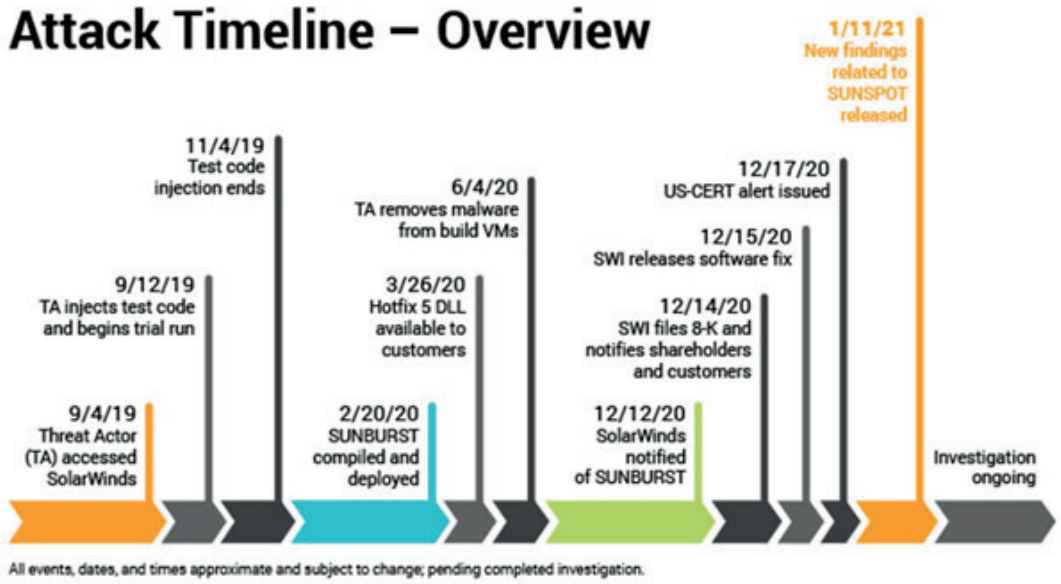
Érdemes megjegyezni azt, hogy a kártevő **szofisztikált DGA** (DomainName Generation Algorithm) algoritmussal rendelkezett, amely azért felel, hogy a domain címeket valamilyen kezdőérték alapján (általában dátum) ad-hoc generálja le, így védekezve a vírusírtó termékek, valamint a rendfenntartó szervek ellen, akik nem tudják lekapcsolni, illetve szűrni a domain címeket.

Miután **sikeresen elvégezte a DNS feloldásokat**, a vírus egy **új végrehajtó szálat nyit** a HttpHelper.Initalize metódussal, amely a továbbiakban a **C2C kommunikációért felelős**. A malware HTTP POST és GET kéréseket használt, emellett ha adatokat szeretne küldeni a külső szervernek, megváltoztatja a HTTP kérés content-type fejlécét „application/json"-ről „application/octet-stream"-re. Az áldozatok könnyebb azonosítása érdekében a kód, egy MD5 alapú userID-t generált a hálózati interfészek MAC címéből, a domain címből, és a regisztrációs adatbázis rekordjából*. Az így előállított azonosítót egy egyedi XOR séma segítségével kódolta. A támadók a rendszer kompromitálása után **különböző malware-eket juttattak** a futtató berendezésre, ezzel elérve az ötödik fázist. Ezeket a TEARDROP és BEACON nevű dropperek segítségével juttatták el, amelyek különlegessége, hogy nem interaktálnak az adattároló egységekkel, nem kerülnek kiírásra a diszkre, hanem rögtön a memóriába töltődnek be. A hatodik fázis, a parancs és vezérlés a már említett C&C szervereken keresztül valósult meg.

Zárásképpen az utolsó fázis, a **megszerzendő adatok kinyerése** és a lehető legtovább tartó **rejtőzködés**, amelyet szintén a lehető legszofisztikáltabb módon valósított meg a kártevő. 10 évvel ezelőtt egy tipikus támadásnál átlagosan 300 nap telt el a kezdete és a felismerés között, napjainkban átlagosan 100 nap. A jelenlegi incidens esetén több mint egy év telt el a felismerésig.

*(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid)

Kármentés



5. ábra: A támadás időrendi sorrendje

Nagyon nehéz egy biztonsági incidens után megszüntetni a fenyegetettséget. Az egyetlen jó megoldás „földig égetni" a meglévő infrastruktúrát és újjáépíteni az alapjaitól. Ezt az üzemeltetők is gyorsan belátták, akik a 2020-as ünnepi szabadságukat feláldozva, **igyekeztek újraépíteni a rendszereket**, de még így sem lehetnek biztosak abban, hogy sikerül teljesen kizárniuk a támadókat. Sok megoldás van, amely segítségével a perzisztens hozzáférés képes túlélni a számítógép és a hálózat újraépítését. Ilyen volt például az NSA támadó kódja is (TS//SI//REL - IRATEMONK), amely merevlemez firmware-jében megbújva biztosított védelmet a távoli hozzáférést szolgáltató káros szoftvernek. Ez a kód a Equation Group program csomagban volt megtalálható, amelyet a vélhetően orosz hackercsapat, a Shadow Brokers 2016-ban ellopott és közzétett, ezért sejthető, hogy az alábbi támadás az SRV készlettárában is fellelhető.

Az amerikai belpolitikai helyzet és az incidens közti összefüggés

Az Amerikai Egesült Államokban 2020. november 3-án megrendezésre került az elnökválasztás. November 7-én Joe Biden átlépte a megválasztásához szükséges elektorszámot, így véglegessé vált, hogy Ő lesz az Egyesült Államok 46. elnöke. December 15-én Amerika teljes figyelmét az elektori választás kötötte le, amelynek következtében az állami szereplőktől **nem kapott elég figyelmet a SolarWinds botrány**. Így fordulhatott elő, hogy 2020 decemberében három különböző forrásból is érkeztek információk az incidenssel kapcsolatban, egyszer Donald J. Trump leköszönő elnöktől, másrészt Joe Biden új elnöktől, továbbá a kongresszus is felszólalt az ügyben. **A felelősség Trump elnököt terhelte**, aki ennek ellenére több napon át sem nyilatkozott a támadásról, végül annyit közölt, hogy lehet Kína áll az ügy hátterében. Eközben a szenátusban egy demokrata jelölt kijelentette, hogy a SolarWinds elleni kibertámadás egyenértékű a háborúval. Biden azt nyilatkozta, hogy Trump elhanyagolta a kiberbiztonságot, illetve Őt okolja, hogy a Belbiztonsági Minisztériumnak (DHS) nem volt akkoriban elnöke. A SolarWinds botrány igen mozgalmas időszakban érte az Egyesült Államokat, a politikusok attól tartottak, hogy ezen incidensen kívül van-e még ellenük folyamatban lévő támadás, amelyről nem tudnak.

A támadás következményei

Nagy valószínűséggel a SolarWinds ellen jogi lépéseket fognak tenni azok a magán és állami cégek, amelyek érintettek voltak a támadásban. Ezek a szervezetek igyekeznek **felmérni** az **okozott károkat** és **meghatározni az adatlopás mértékét**. A nemzetközi jog és a diplomácia területén megkezdődtek a szankciók megfogalmazása, válaszlépésre is lehet számítani, de hogy milyen jellegűre, azt még nehéz lenne kitalálni. Barack Obama törekvései, amelyek az USA-Oroszország kapcsolatot próbálták javítani, végképp szertefoszlottak. Az egyik legsúlyosabb kérdés, hogy egy nemzetközi kibertámadásról miért egy privát kiberbiztonsági cégtől kell értesülnie a világnak?

Az incidenst nem egy egyszerű sablonos vírus támadásként kell értelmezni, hanem egy rendkívül összetett, jól megszervezett, nagy költségvetésű, **világméretű kémtevékenységként**. Hasonló támadásokat technikai oldalon nagyon nehezen lehet megfogni és azt is be kell látni, hogy a kibertérben történő támadásoknak a való életben is következményei vannak. Ez az incidens remek példa arra, hogy miért érdemes **védekezés alapú stratégiára** építeni egy nemzet kiberkompetenciáját, valamint szorosabb információmegosztást szorgalmazni az állami és gazdasági szereplők között. A biztonság megfelelő biztosításának mellékhatásaként felmerülhet a jelenlegi szabadságjogok korlátozása, illetve az egyének feletti állami kontroll.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36(1)325 7672

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Kibertámadás!
podcast

2022