A Solarwinds incidens

Kiberbiztonsági elemzés

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT Fortes fortuna adiuvat

Tartalom

Bevezetés

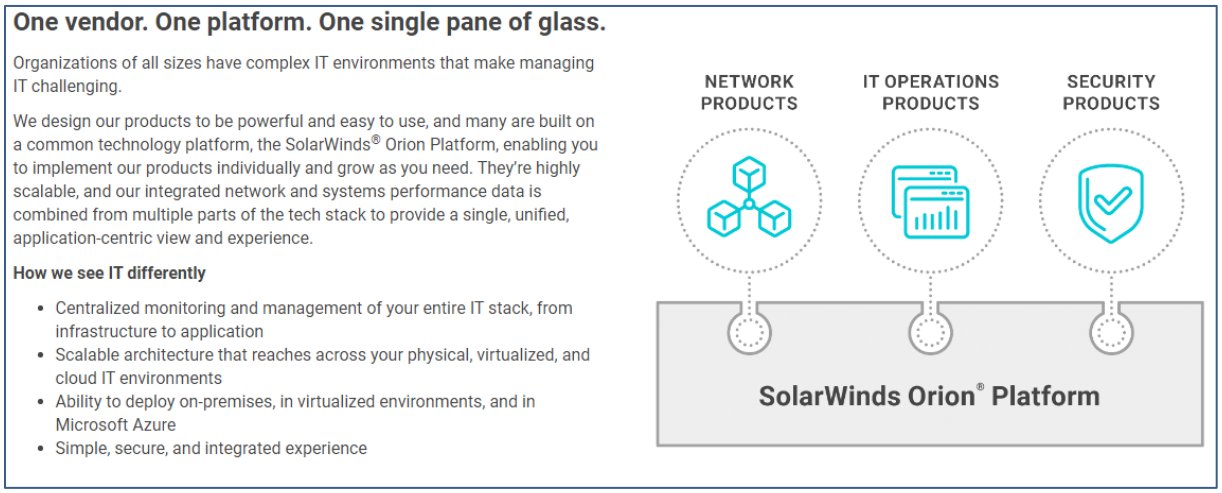
2019 végén, 2020 elején kirobbant világjárvány hatalmas változást hozott az informatika világában. A fertőzés terjedésének lassítása érdekében törekedett mindenki minimalizálni a fizikális kontaktust és így elkerülni a megfertőződést is. Az internet, amelynek legfőbb célja a kommunikáció különböző informatikai 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.

Incidensek

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 ügyfele használja.

1. ábra: Solarwinds cég logója

Az Orion-t a teljes informatikai infrastruktúra központi menedzselésére tervezték, rendelkezik hálózati forgalom, szerverek és szolgáltatások monitorozására is alkalmas modulokkal. Ezt a terméket nem csak a multi cégek használták a több ezer számítógéppel és szerverrel rendelkező infrastruktúrájuk kordában tartására, hanem amerikai állami szervezetek is. Ezek közé tartozik az amerikai külügyminisztérium, belbiztonsági minisztérium, energiaügyi minisztérium, három állam, emellett a Nemzeti Nukleáris Bizottság, Kiberbiztonsági és Infrastrukturális Ügynökség, Egészségügyi Minisztérium és a Kereskedelmi Minisztérium is. A United States Computer Emergency Readiness Team (US-CERT) által fejlesztett és a United States Department of Homeland Security által üzemeltetett EINSTEIN hálózati forgalom monitorozó rendszer sem jelzett kártékony aktivitást, minden állami minisztérium és ügynökség rendelkezik egy ilyen berendezéssel.



2. ábra: Orion platform jellemzői

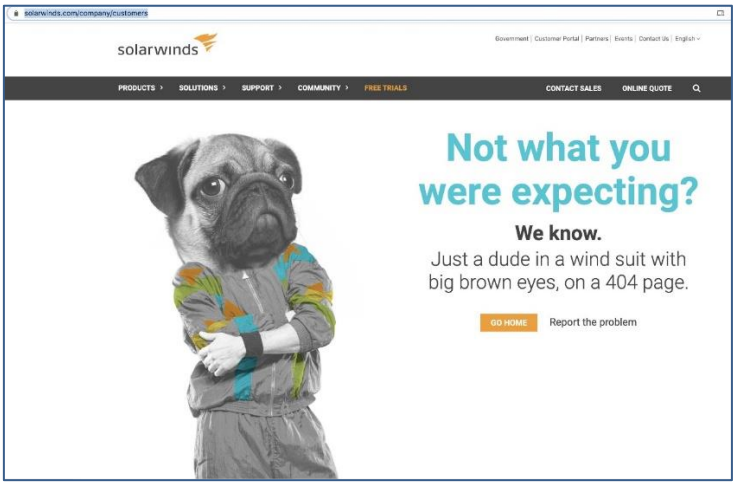
2020 márciusában az APT29 vagy CozyBear nevet viselő hacker csapat, akik feltehetőleg az Orosz SRV-nek dolgoztak (korábban KGB-ként ismerhető), elhelyeztek egy hátsó kaput az Orion platform szoftver frissítései között. 2019-ben egy biztonsági kutató bejelentést tett a SolarWinds cégnél, hogy a frissítésért felelős szolgáltatásuk hitelesítése gyenge jelszóval van

védve(solarwinds123). A bejelentéssel nem foglalkozott érdemben a cég. Azok a felhasználók, akik március és június között letöltötték a frissítését a szoftvernek akaratlanul is hozzáférést adtak az SRV-nek a teljes hálózatukhoz. Ezt supply-chain (ellátási lánc) támadásnak nevezik, mert ez támadni kívánt szervezet beszállítóját célozza, ezáltal a beszállító összes ügyfeleit is. A támadást sokáig egyetlen szervezet sem detektálta, így közel fél évig szabad bejárást biztosított a hacker csapat 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 szerződéses, illetve szerződés nélküli alapon. Az utóbbi a bűnszervezetekbe való beépülés és megtámadásuk célját szolgálja, amely kérdéseket vethet fel jogi szempontból is.

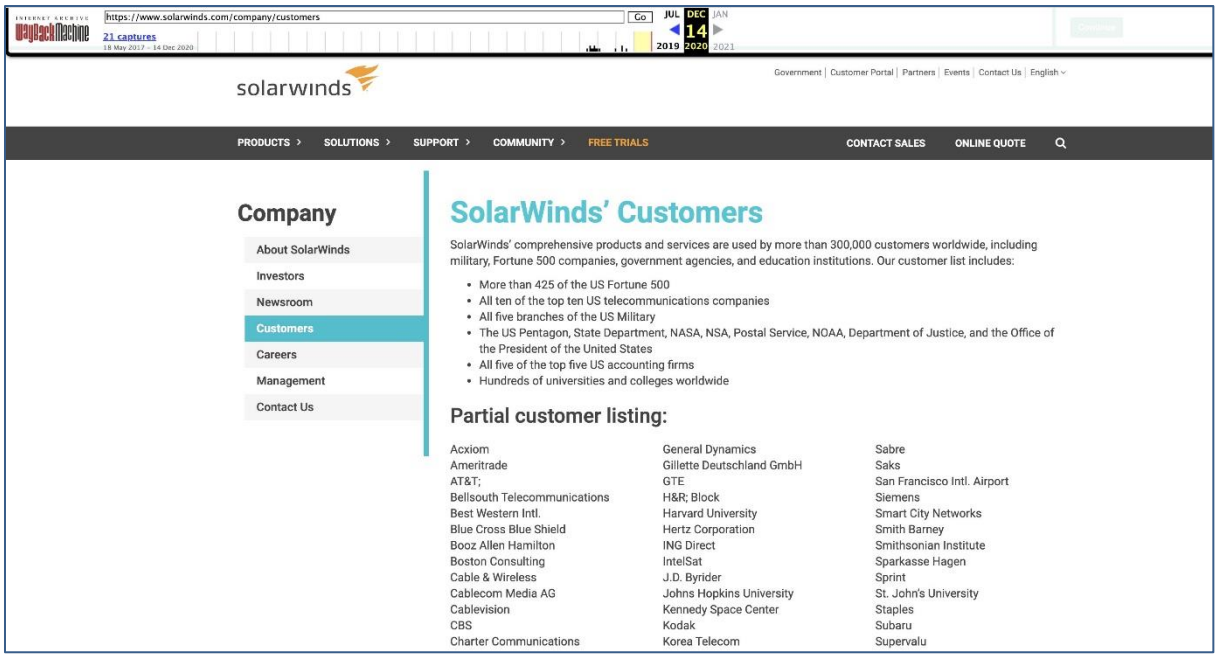
Ez a csapat rendelkezett egy kisebb arzenállal felérő támadó kóddal, melyek sérülékenységek kihasználására alkalmasak, nem beszélve a 0. napi támadókódokról. 2020. december 8.-án a cég bejelentette, hogy állami támogatással rendelkező ismeretlen hackerek bejutottak a FireEye hálózatába és ellopták a 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 szabálycsomagot (https://github.com/fireeye/red_team_tool_countermeasures), 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.



3. ábra: Eltávolított ügyféllista

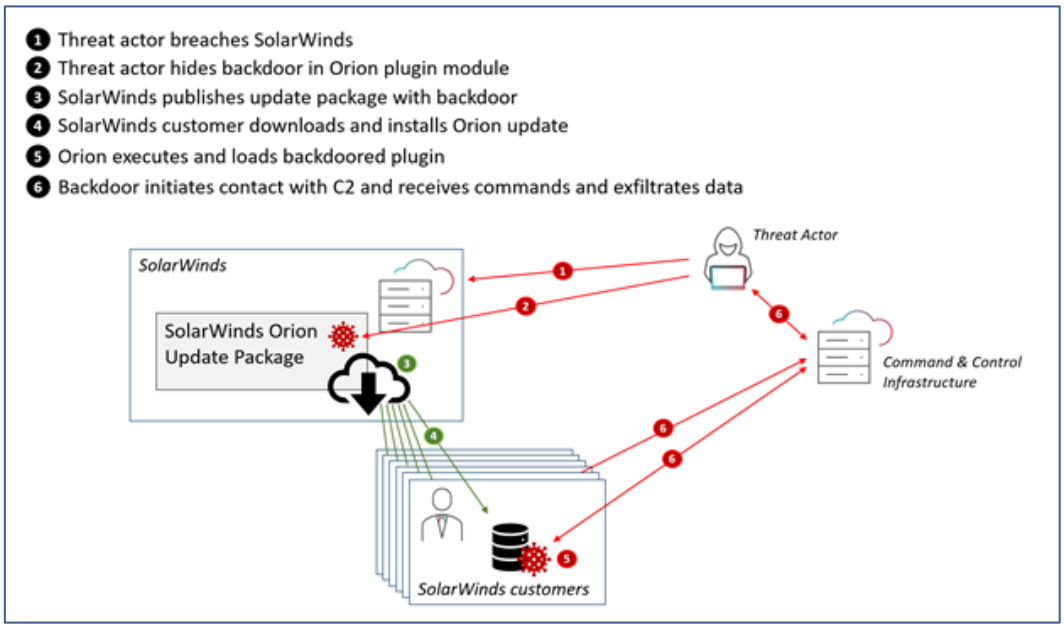
Az Internet Archive alapítvány által működtetett weboldalak tükrözésével foglalkozó szolgáltatás viszont elmentette az oldal eredeti tartalmát.



4. ábraWayBackMachine által megrzött 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



5. ábra: Támadás folyamata

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, a SolarWinds cég ideális célpont, 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. 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 egyértelműen 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 (Sorozatszám: 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed) digitális alá volt írva. A komponens tartalmazott egy backdoor-t, amely egy távoli szerverrel kommunikált.

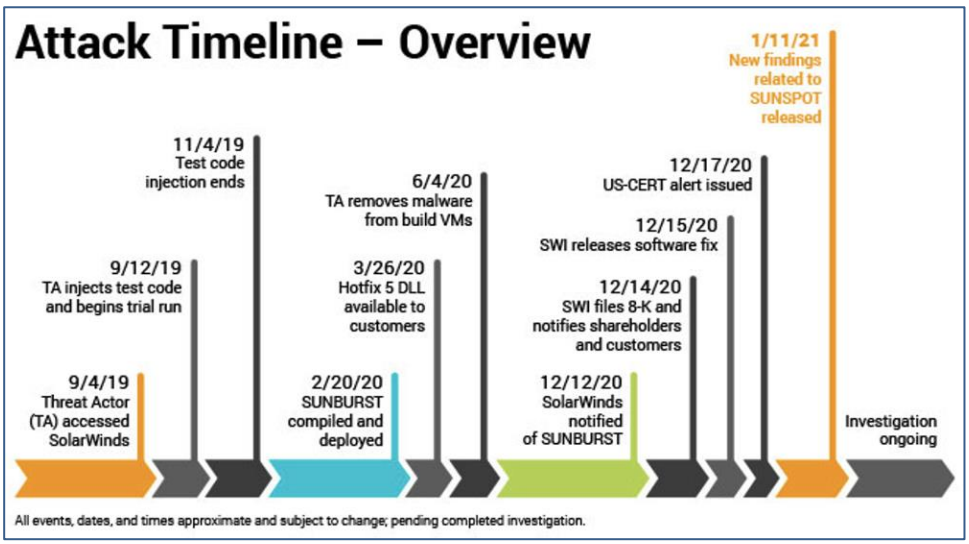
A FireEye cég SUNBURST névre keresztelte el a komponenst és kiadott egy nyílt forrású detektáló készletet, amely segítségével a nagyobb IPS/IDS rendszerek és vírusírtók is fel tudták ismerni a támadás jelenletét a belső hálózatokon, illetve a már települt kártevő jelenlétét a számítógépeken. (https://github.com/fireeye/sunburst_countermeasures) 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. 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 és 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 (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid). Az így előállított azonosítót egy egyedi XOR séma segítségivel is 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.

Kármentés



6. ábra: Támadás időbeni lefolyása

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 2020 ünnepi szabadságukat feláldozva igyekeztek a rendszereket újraépíteni, 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.

Amerikai belpolitikai helyzet és az incidens közti összefüggés

November 3.-án megtörtént az elnökválasztás Amerikában. November 7.-én Joe Biden átlépte a megválasztásához szükséges elektorszámot, így véglegesen eldőlt, hogy ő lesz az Egyesült Államok 46. elnöke. A választás napja és a szenátusi választás közötti időszakot béna kacsának nevezik, mivel az leköszönő elnök, akit nem választottak újra, már nem rendelkezik már akkora hatalommal, mint amit az utóbbi 4 évben tudott gyakorolni. Washingtonban december 15.-én Amerika teljes figyelmét az elektori választás kötötte le, melynek következménye, hogy nem kapott nagy érdeklődést az állami szereplőktől ebben az időszakban ez az incidens. Decemberben három különböző kommunikációt kaptunk az incidenssel kapcsolatban. Egyet Donald J. Trump leköszönő elnöktől, egyet Joe Biden új elnöktől, aki már a tranziciós időszakban megkapta a napi nemzetbiztonsági jelentéseket, melyek az elnöknek járnak, emellett a kongresszus is felszólalt az ügyben. A felelősség Trump elnököt terhelte, aki ennek ellenére nem nyilatkozott a támadásról több napon keresztül, majd annyit közölt, hogy lehetséges, hogy Kína állhatott az ügy hátterében.

Emellett megnyugtatás végett bejelentette, hogy minden rendben van, „everything well under control”. Közben már a szenátusban egy demokrata jelölt kijelentette, hogy ez a tett egyenértékű a háborúval. Biden azt nyilatkozta, hogy Trump elhanyagolta a kiberbiztonságot, illetve Trump hibája az is, hogy nem volt a Belbiztonságnak elnöke (DHS). Jelenleg az a politikai harc zajlik, hogy ki tud ebből politikai tőkét csinálni. Roppant mozgalmas időszakban érte ez az incidens az Egyesült Államokat, elkezdtek félni attól a politikusok, ha ilyen történhetett velük, akkor van-e még olyan folyamatban lévő támadás, amelyről nem tudnak.

A támadás következménye

Arra mindenképpen lehet számítani, hogy a SolarWinds ellen jogi lépéseket fognak tenni azok a magán és állami cégek, melyek a támadás áldozataivá váltak. Most minden érintett cég és állami szerv próbálja felmérni az okozott kárt és kitalálni 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. A Barack Obama törekvései, melyek az USA-Oroszország kapcsolatát próbálták javítani végképp szertefoszlottak. Az egyik legsúlyosabb kérdés, hogy egy nemzetközi kibertámadásról miért egy privát kiberbiztonsági cégtől kell értesülnie a világnak? Rengeteg támadás volt és van folyamatban a világon, 2010-ben USA és Izrael megtámadja az Iráni nukleáris programot, 2012-ben Irán megtámadja a Saudi nemzeti olaj vállalatot, 2014-ben Észak Korea megtámadja a Sony céget, Oroszország megtámadta az Ukrán elektromos hálózatot 2015-ben és 2016-ban. Oroszország megtámadta az amerikai elektromos hálózatot, Amerika erre visszatámadta az orosz villamos hálózatot.

Az incidenst nem egy egyszerű sablonos vírus támadásként kell felfognunk, hanem egy rendkívül összetett, jól megszervezett és nagy költségkerettel rendelkező világ méretű kémtevékenységként. Hasonló támadásokat technikai oldalon nagyon nehezen lehet megfogni. Be kell látnunk, hogy ezek a kibertérben történő támadásoknak a való életben következményei vannak! Amerika hibáján tanulhattuk meg, hogy elengedhetetlen a védekezés alapú stratégiára építeni a kiberkompetenciánkat. A jövőbeni hasonló akció kivédése érdekében a cégek és állami szereplők között szorgalmazni kell az szorosabb információmegosztást, a helyi és az állami rendszerek, adatbázisok összekapcsolását. A biztonság megfelelő biztosításának mellékhatásaként felmerülhet a jelenlegi szabadságjogok korlátozása, illetve az egyének feletti állami kontroll.

Kapcsolat

Nemzeti Kibervédelmi Intézet (NKI)

E-mail: titkarsag@nki.gov.hu
Telefon: +36 (1) 336 4840
Fax: +36 (1) 336 4886

Posta: **1399 Budapest,**
62. Pf. 710.

Nemzeti CSIRT

Web: https://nki.gov.hu
E-mail: team@nki.gov.hu
Incidens-bejelentés: csirt@nki.gov.hu
PGP: 601B 71A8 338D 5181

0-24h ügyelet: +36 (1) 336 4833

Eseményészlelés (EWS, Honeypot, CTI)

Web: https://nki.gov.hu/edt
E-mail: edt@nki.gov.hu
PGP: 88A2 E465 BF51 AD58
EWS: ewscsatlakozas@nki.gov.hu
Honeypot: honeypot@nki.gov.hu

Hatóság

Web: https://nki.gov.hu
E-mail: info@neih.gov.hu
PGP: 0x2938f849