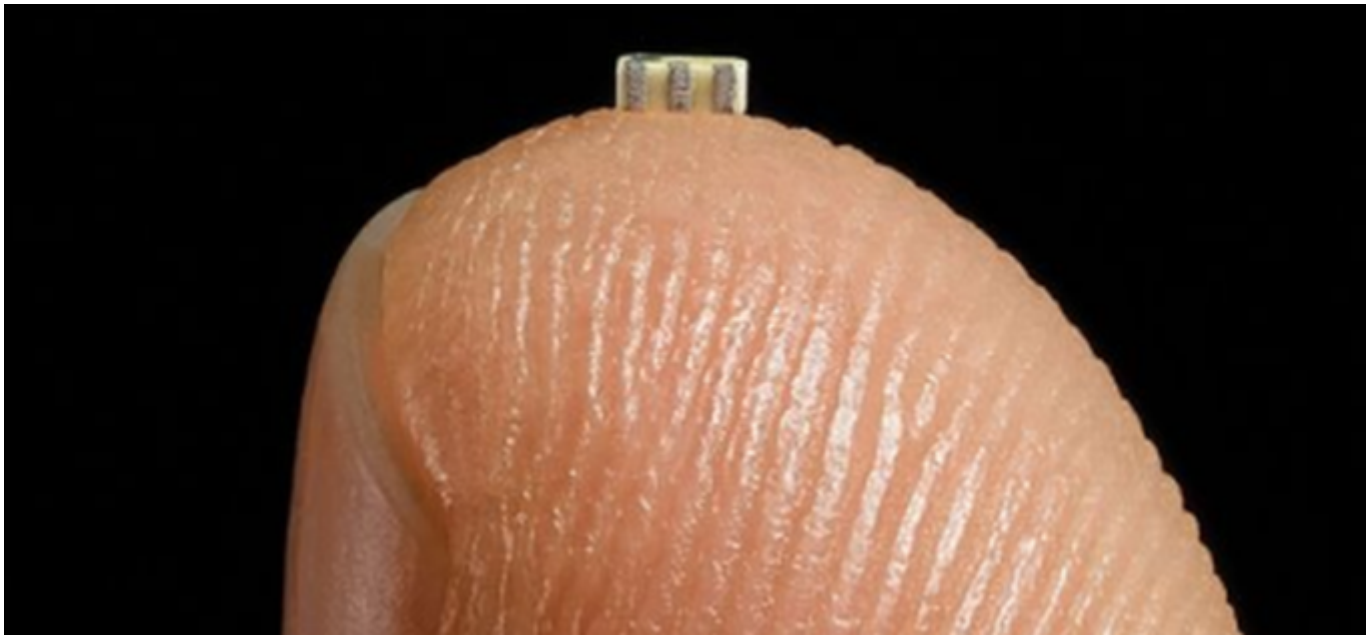
A Supermicro történet

A **Bloomberg** által feltárt történetben egyelőre minden érintett hevesen tagad. A sértettek és a *„gyanúsítottak”* egyaránt és egybehangzóan állítják, hogy *nem történt semmi, kéretik továbbfáradni, nincs itt semmi látnivaló*. Csak az a gond, hogy sokat számára – számomra is – ez a nagy mentegetőzés felér egy olyan beismeréssel, ami az igazán penetráns ügyeket szokta szegélyezni, hogy mást ne említsek, az ezen a blogon már ismertetett Stuxnet ügyet például.



Szóval, tegyük fel, hogy a Bloomberg-nek igaza van (az eredeti történet itt olvasható), és az általa leírtak tényleg megtörténtek. Ezt feltételezni már csak azért sem nehéz, mert egyrészt a Bloomberg ritkán nyúl mellé, másrészt a történet teljesen hihető, illeszkedik a kínai totális megfigyelések sorába (erről is már volt szó), és technikailag megvalósítható. Ráadásul a feltárt történet már három éve történt, így inkább az a meglepő, hogy eddig hogyan tudták mindezt eltitkolni.

2015-ben az Amazon egyik vállalkozása, az **Amazon Web Services** (**AWS**) felvásárolta az **Elemental Technologies** nevű, streaming videók képtömörítési eljárásával foglalkozó startupot. Úgy vélték, ezek az eljárások segítenek nekik például az olimpiai közvetítések átvitelében, de jó hasznukat vennék a nemzetközi űrállomással való kommunikáció optimalizálásában vagy a CIA drónfelügyeleti rendszereinek a képátvitelénél.

Mivel a technológiát nem kis részben kényes adatok átvitelére szánták, felkérek egy harmadik céget, hogy világítsa át a projektet és tárja fel a technikai problémákat. Az első vizsgálatok érdekes összefüggéseket tártak fel az Elemental által alkalmazott alaplapok, a **Super Micro Computer Inc.** tulajdonosi hátterével kapcsolatban, így magukat az alaplapokat is egy szigorúbb vizsgálatnak vetették alá.

A vizsgálatok összevetették a tervezett alaplapokat a leszállítottakkal, és egy rizsszem méretű mikrochipet találtak, ami nem volt része az eredeti kialakításnak. Az Amazon azonnal bejelentette a felfedezését az amerikai hatóságoknak, és a hír tényleg bizonyos körökben nagyot robbant.

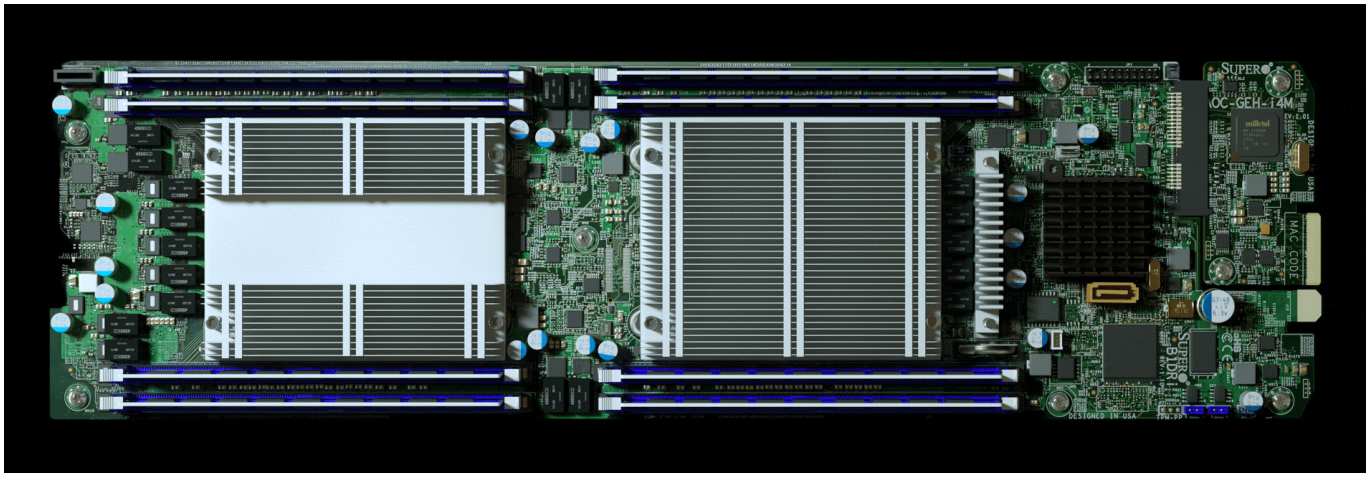
Gyorsan feltárták ugyanis, hogy az Elemental érintett szerverei szinte minden, állambiztonságilag fontos területen megtalálhatók; a Védelmi Minisztérium (*Department of Defense* -**USDOD**)

adatközpontjaiban, a drónok képátviteli hálózataiban vagy a hadihajók fedélzeti hálózataiban. Az elkövetkező három év egyfelől a *„tűzoltással”* telt, hogy az érintett szervereket kivonják a rendszerből, másfelől a történtek feltárásával.

A kutatómunka eredményeként felismerték, hogy a chip technikailag egy hátsó ajtó a szervereken. Sok vírus (malware, trojan, és egyéb behatoló) malware] is képes erre a kunsztra, de a szoftveres fertőzések hatékonyan feltárhatók és kezelhetők, míg a hardveres megoldás – mivel integráns része az alaplapnak – szinte észrevehetetlen. Az kém-chip (nevezzük a továbbiakban így, bár ez az elnevezés némileg pontatlan) külső parancsok hatására be tud avatkozni a CPU és a gyorsítótár közötti kommunikációba, és módosítani tudja például a CPU által végrehajtott parancsok sorrendjét.

Ezzel például el lehet érni, hogy az adott szerveren futó, és biztonságosnak tekintett Linux operációs rendszer jelszóellenőrző eljárásának *„kiiktatásával”* kívülről is hozzá lehessen férni titkos tartalmakhoz, természetesen jelszavak nélkül. A kém-chip ezen kívül alkalmas titkosítási kulcsok lopására, blokkolhatja a biztonsági frissítéseket, ellenőrizetlen hozzáférést biztosíthat az internethez.

Mivel a kém-chipeket úgy tervezték, hogy időről időre bizonyos távoli gépekkel felvették a kapcsolatot további utasítások fogadása céljából, így ezeknek a kapcsolatfelvételeknek a visszakövetésével sikerült a (potencionálisan) lehallgatott gépek hálózatát feltárni.



Az amerikai nyomozók megállapították, hogy mintegy 30 cég érintett ebben a kémtörténetben, a már megismert (és a botrányt kirobbantó) Amazonon kívül az **Apple** neve is előkerült – persze ezt ők is váltig tagadják. Ráadásul, híresztelések szerint az almás cég már 2010-ben felfigyelt a Supermicro-s alaplapok furcsa hálózati tevékenységére, de anélkül, hogy erről bárkit is értesítettek volna, házon belül *„kezelték”* a problémát; lecserélték az érintett gépeket. Két vezető bennfentes szerint erről aztán azért az FBI-t is tájékoztatták.

Becslések szerint a kereskedelmi forgalomba kerülő mobiltelefonok alkatrészeinek 75%-át és a számítógépek 90%-át kínai gyártók állítják elő. A Supermicro gyára az USA-ban, a San Jose repülőterétől északra található. A vállalatot egy egykori tajvani mérnök, **Charles Liang** alapította 1993-ban.

Az elképzelés az volt, hogy a Szilikon-völgyi igényeket a helyi összeszerelő-üzem kínai alkatrészekből szerelt gépekkel elégítette ki. Napjainkban a Supermicro több szerver-alaplapot terít a piacon, mint bárki más, és mindezt úgy, hogy a termelés legnagyobb része Kínában (vagy legalábbis a térségben) zajlik. Ráadásul a san jose-i gyárban is az ott dolgozók javarészt kínaiak vagy tajvaniak; a gyáron belüli hangosbeszélős hívások is minden esetben angolul és aztán mandarin nyelven hangoznak el.

A nyomozók szerint a chip-et legnagyobb valószínűséggel a kínai Népi Felszabadítási Hadsereg hardveres támadásokra szakosodott egysége fejlesztette ki. Ennek a csoportnak a létezését – talán nem meglepő módon – a kínaiak soha nem ismerték el.

Egy – az ügyben a Bloombergnek szivárogtató tisztviselő erről úgy nyilatkozott: *„Ezt a fickót (aki a kínaiakat ez ügyben „képviselte") hosszabb ideje nyomon követjük, mint amennyit beismerhetnénk ez ügyben."* Ez a kínai speciális egység a kiemelt prioritású ügyekre koncentrál, azaz elsősorban a kereskedelmi technológia és az ellenséges katonai technológiák után kémkednek és fejlesztenek kémkedésre alkalmas technológiákat.

Mindenesetre az ügy kipattanását követően az amerikai nyomozóhatóság *„rászállt"* a Supermicro beszállítói láncolatára, és négy olyan kínai/tajvani beszállítót is azonosítottak, ahol a kém-chip belekerülhetett a gyártásba, és feltárták ennek a *„fejlesztésnek"* a hátterét.

Ezekhez a gyártókhoz a kínai kormány által delegált „kapcsolattartók" érkeztek. Eleinte csak a tervezési folyamatok dokumentációját *„kérték ki"*, majd jelezték, hogy hol és hogyan kell változtatni a kiviteli terveken. A gyárigazgatókat az ügynökök korrupcióval, vagy adott esetekben fenyegetésekkel – például szigorított, és a munkát ellehetetlenítő ellenőrzésekkel – vették rá az együttműködésre.

A kínaiak kémkedési törekvései nem újszerűek; a **Huawei** és a **ZTE** esetén a kormányszervek már korábban is figyelmeztettek az efféle kínai kormányzati beavatkozásokra – ezt a gyanúsítást persze mindkét gyártó hevesen elhárította.

A botrány kibontakozását követően a Supermicro csillagának is leáldozott az USA-ban. Az eladásai visszaesése mellett a számviteli szabályok megsértése okán (*„elfelejtették"* kiadni a negyedéves és éves beszámolóikat) – törölték a papírjaikat a Nasdaq-ról.

Nagyon valószínű, hogy ez a botrány nem egyedülálló. Több szakértő is egyetértett abban, hogy a kém-chip elhelyezése a nyomtatott áramkör felületén meglehetősen primitív megoldás volt, még ha törekedtek is arra, hogy az alkatrész inkább tűnjön bármi más passzív alkatrészek, csak ic-nek ne.

Lehetőségük lett volna például a többrétegű nyomtatott áramköri rétegei közé rejteni a chip-et, ott aztán tényleg senki nem vette volna észre, vagy bármely más alkatrészbe, például egy (másik, de tervezett) ic-be integrálni azt. Persze ezek a feltevések egyáltalán nem megnyugtatóak, hiszen ki tudja, hogy mennyi más Kínában gyártott berendezés tartalmaz még jól (vagy jobban) elrejtett kém-chip-eket.

Ráadásul, az elnevezés, a kém-chip sajnos arra utal, hogy ezek az alkatrészek csak kémkedésre valók, pedig nem. Ezek olyan hátsó-ajtók (backdoor), amiken keresztül a gépek működésébe is be lehet avatkozni, adott esetben például távirányítással teljes országnyi infrastruktúrákat lehet a segítségével lebénítani.

Ez a botrány alapjaiban kérdőjelezi meg a jelenlegi ellátási láncokat: **Érdemes e továbbra is a kínai kitettséggel és fenyegetéssel veszélyeztetni az infrastruktúráinkat?**

Update1

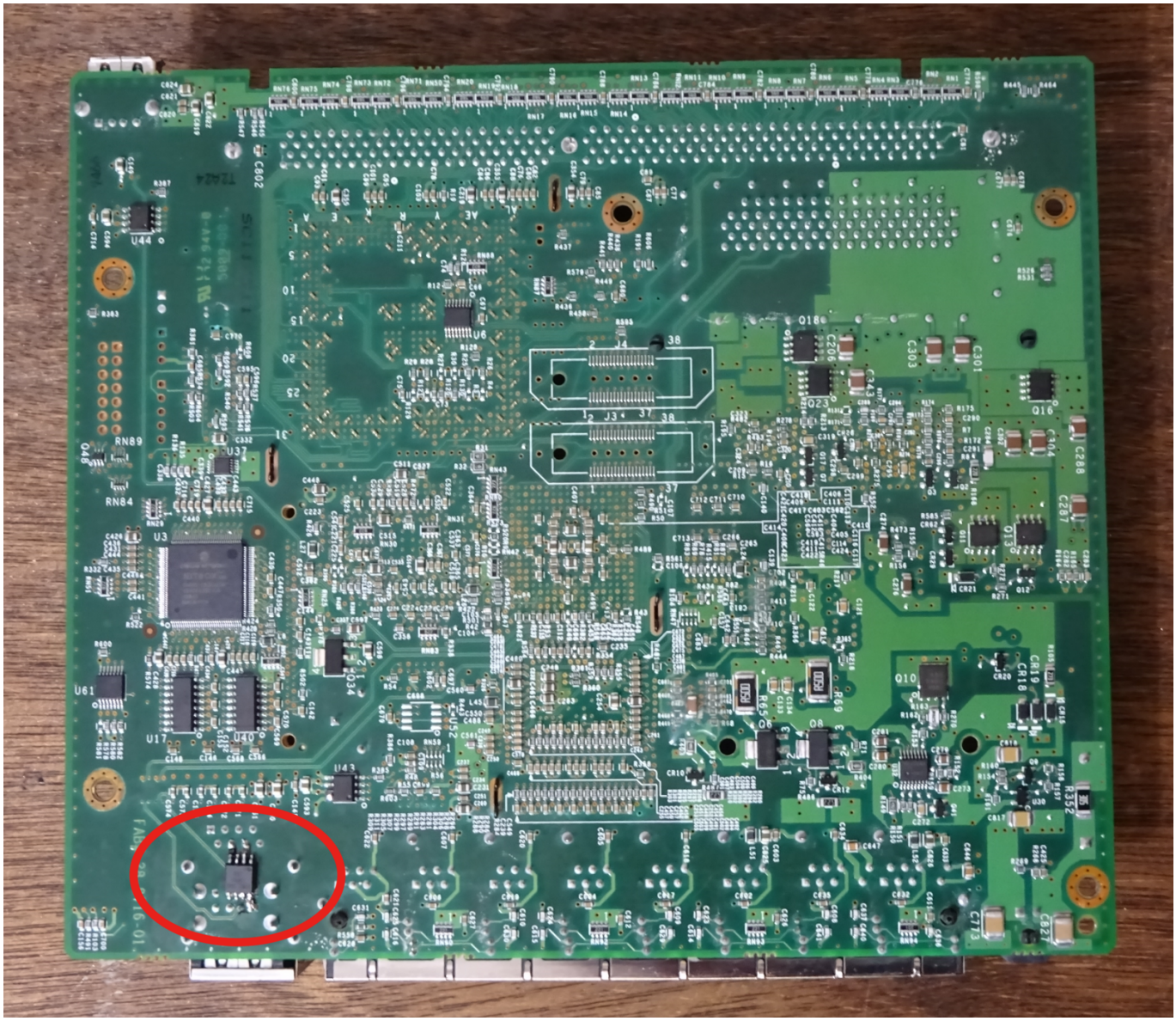
Nyilván mi, mezei kívülállók soha nem fogjuk megtudni az igazságot, hogy ez a történet csak kitaláció vagy maga a valóság, de néhány fejlesztő egy másik irányból közelítette meg a történteket, és

feltették a kérdést: **Meg lehet valósítani ezt a hackelést egyszerű, „bolti” eszközökkel?**

Az eredményről **Monta Elkins** biztonsági szakértő számolt be a stockholmi **CS3sthlm biztonsági konferencián** (2019.10.21-24.). Ő egy **Attiny85** chipet használt az alkalmazásához, melyet egy 3 dolláros Arduino Digispark fejlesztőpanelről forrasztott le.

Ez az IC azért még messze nem rizsszem méretű, mint a történetben, de első próbálkozásnak azért ez is megtette. Elkins az előadásában utalt arra, hogy választhatott volna sokkal kisebb IC-t is, de az Attiny-t könnyebb volt programozni.

A lenti képen a chippel meghekkelt Cisco (ASA 5505) tűzfal alaplap látható; nem biztos, hogy bárkinek, aki nem ezt a változást keresi, feltűnne a dolog:



Elkins úgy programozta az IC-t, hogy amint a tűzfal elkezd bootolni az adatközpontban, az elindít egy jelszó-helyreállítási funkciót és létrehoz egy új rendszergazdai fiókot, ezzel hozzáférést biztosít a tűzfal beállításaihoz. Előadását így zárta: *„Úgy lehet megváltoztatni a tűzfal beállításait, hogy az adminisztrátor erről nem értesül. Megváltoztathatom a tűzfal konfigurációját, bármit megtehetek vele.”*

Ráadásul **Trammell Hudson**, független biztonsági szakértő már korábban is igazolta, hogy azon a helyen, ahol a Bloomberg írása feltételezte a kínai kém-chipet a super micro-s alaplapon, egy olyan újraprogramozható logikai áramkör található, amivel egy rosszindulatú lehallgatás megvalósítható.

Mindenesetre Monta Elkins egy három dolláros IC-vel, egy forrasztópákával, meg némi programozással megoldotta azt a hozzáférést, amit az NSA szerint a kínai szakértők technikailag nem tudtak volna megvalósítani.

Ők vagy a kínaiakat, vagy minket néznek hülyének..

Ajánló

Hasonló jellegű bejegyzéseket a **cyberwar** tag alatt talál:

- A Davis-Besse atomerőmű esete a vírussal 2025/07/20 08:26
- A Stuxnet sztori 2025/07/20 08:26
- A Supermicro történet 2025/07/20 08:26
- A Trans-Szibéria gázvezeték 1983-as robbanása 2025/07/20 08:26
- A Világ valódi csodái 2025/07/20 08:26
- Krétával és palatáblával a zsarolóvírus ellen 2025/07/20 08:26
- Xiongmai sztori 2025/07/20 08:26

Kedves olvasóm! Ha már idáig eljutottál az olvasásban, talán joggal feltételezhetem, hogy nem volt teljesen érdektelen számodra ez a bejegyzés. Jaj, le ne ixelj még; nem pénzt akarok tarhálni.

Pusztán annyit kérek, hogy ha van olyan ismerősöd, akivel jót tudnál vitatkozni az itt leírtakról, vagy csak simán megosztanád vele, kérlek, ne késlekedj!

Továbbra is keresek megjelenési lehetőséget az írásaim számára. Ha esetleg van ötleted, osszd meg velem! Elérhetőségeim az Impresszumban találhatók.

A passport.blog jelenlegi egyetlen megjelenési lehetősége a Facebook. Ha értesülni szeretnél az új bejegyezésekről, kövesd a Bolyongó Facebook oldalt.

Ha szeretnéd a bejegyzést kinyomtatni, vagy önálló formában menteni, ennek a legegyszerűbb módja a PDF formába konvertálás. Ezt a jobb oldali, fentről negyedik (Adobe) ikonnal teheted meg.

Eddigi bejegyzések a bolyongó.hu-n

Az összes bejegyzés ABC-be rendezett indexe itt található. A blog helyekhez köthető bejegyzései a google.maps térképen is megtalálhatók: A világ valódi csodái. A mostanában a blogon megjelent írások a főoldalon jelennek meg.

2025/07/20 08:26

Forrás

A bejegyzést a Bloomberg alábbi cikke alapján írtam:

Bloomberg: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

Update1

Wired: Planting Tiny Spy Chips in Hardware Can Cost as Little as $200
computing.co.uk: Tiny $2 spy chip can be added to IT hardware, claims security researcher Monta Elkins

tech, vírus, lehallgatás, kémkedés, backdoor, cyberwar, 2018, USA, Kína, Amazon, Apple, Supermicro, Bloomberg, AWS, Elemental Technologies, CIA, tech, Super Micro Computer Inc, USDOD, kém-chip,

San Jose, Charles Liang, Szilikon-völgy, Huawei, ZTE, biztonság, CS3sthlm, Monta Elkins, Attiny85, Cisco ASA 5505, Trammell Hudson, tűzfal, hack, botrány, kici oco, hardver

Bejegyzésmegtekintések száma: 284