HUNCERT PROBE

ismertető és útmutató

A programról

A PROBE program, valamint az ennek keretében az önkéntesen és térítésmentesen résztvevő támogatók (tagok) által saját hálózatukban elhelyezett szonda állomások célja a hazai interneten tapasztalható hálózati biztonsági trendek rögzítése és elemzése, a Hun-CERT incidens-érzékelési képességének javítása, illetve a programban részt vevő hálózati rendszereket üzemeltetők és internet szolgáltatók számára átfogó, illetve saját hálózatuk szempontjából releváns és aktuális biztonsági információk elérhetővé tétele.

A PROBE eszköz – néhány, az alábbiakban részletezett technikai kivételtől eltekintve – **teljesen passzív**, vagyis kimenő hálózati forgalmat nem kezdeményez, pásztázást sem a helyi hálózat, sem az internet irányába nem végez. A PROBE kialakítása és üzemeltetése során elsődleges szempont, hogy az elhelyezését önkéntesen biztosító gazda hálózatot az eszköz semmilyen műszaki vagy jogi megfontolásból eredően **nem veszélyeztetheti,** illetve nem gyűjthet közvetlenül a helyi hálózatról származó információkat.

A PROBE eszköz semmilyen valós, nyilvános internetes **szolgáltatást nem nyújt**, lehallgatást („sniffing”) nem végez, így az általa begyűjtött információk csak az **aktívan és kéretlenül** hozzá kapcsolódó **külső támadók**, jellemzően automatizált mechanizmusok, által **szándékoltan megadott**, szokványos esetben is naplózásra kerülő, a programban résztvevő támogatók által a program számára felajánlott, saját hálózati erőforrásaikról (vagyis a PROBE eszköz nyilvános IP címéről) **önkéntesen megosztott** adatok.

Megjegyzés: a PROBE hardver eszközökben elhelyezett WiFi hálózati adapter jelenleg inaktív, ezt csak a programban részt vevők explicit engedélyével aktiváljuk. A WiFi adapter az eszközből szabadon eltávolítható, azonban ez esetben annak visszaszolgáltatását kérjük.

Rólunk

A magyar Internet Szolgáltatók Tanácsa (ISZT), valamint a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézete (MTA SZTAKI) által támogatott, non-profit Hun-CERT csoport immár több, mint 15 éve hálózatbiztonsági incidensek felderítésével, elemzésével és kezelésével, valamint a felhasználói biztonsági tudatosság növelése irányában tett erőfeszítéseivel szolgálja hazai Internet biztonságát.

Tevékenységünk során a kölcsönös bizalmon alapuló információmegosztás és a függetlenség alapelvei mellett magas szintű kutatás-fejlesztési eredményeinkre támaszkodunk.

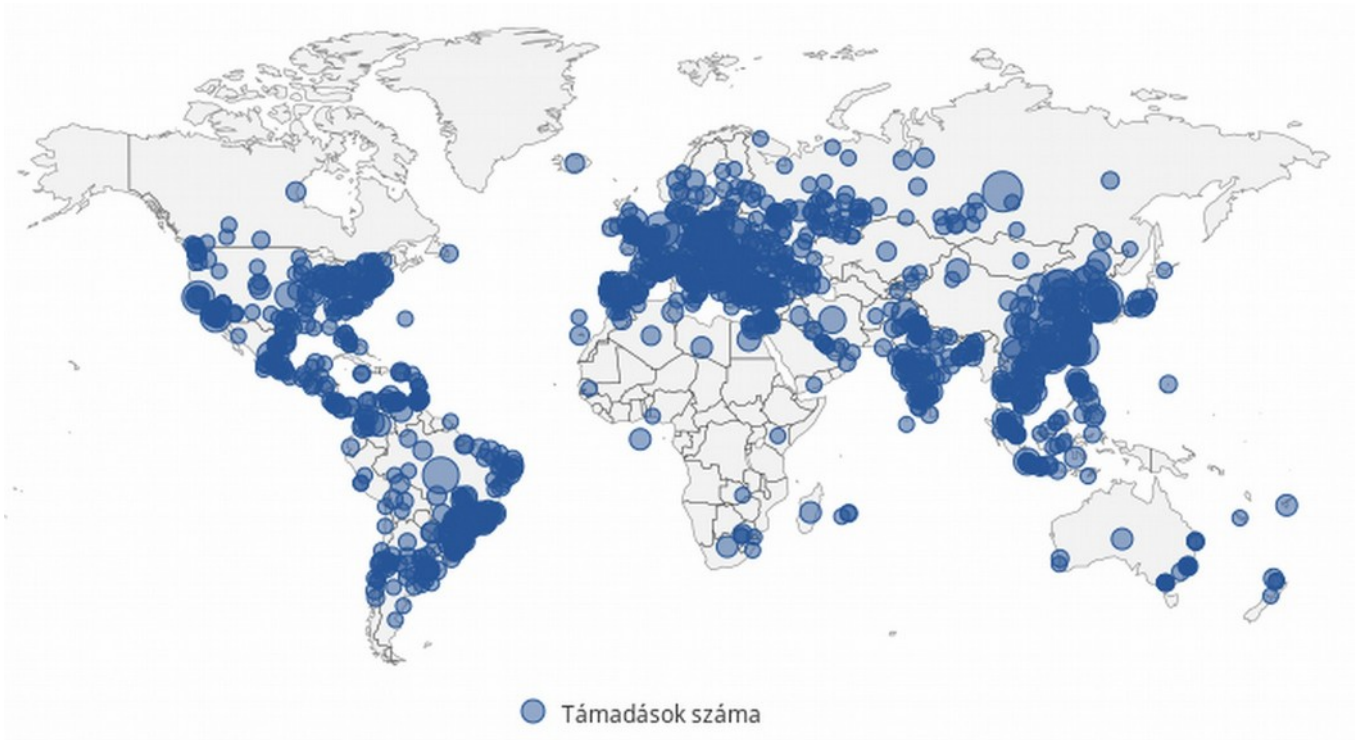
A begyűjtött adatok hasznosítása – adatkezelési nyilatkozat

A PROBE program során begyűjtött adatokat a Hun-CERT kizárólag az alábbi célokra használja fel:

- A program nyilvános weblapján (https://hab.cert.hu) trend jellegű adatok, havi és éves grafikonok megjelenítése (forrás és cél IP címek megadása nélkül). A megjelenített adatokból semmilyen módon nem lehet következtetni a PROBE eszközök elhelyezkedésére, így a programban részt vevő támogatókat érintő egyedi trendek és események sem azonosíthatók.
- A programban részt vevő támogatók (tagok) számára, azonosítást követően elérhető weblapon szűrhető összesített grafikonok, a hazai internetet támadó külső állomásokra és tevékenységekre vonatkozó toplisták megjelenítése, a nyilvános felületen elérhetőnél bővebb adattartalommal (például: támadások esetén külső forrás IP cím megjelölésével). A megjelenített adatokból semmilyen módon nem lehet következtetni a PROBE eszközök elhelyezkedésére, így a programban részt vevő támogatókat érintő egyedi trendek és események sem azonosíthatók.
- A programban részt vevő támogatók (tagok) számára, azonosítást követően elérhető weblapon a saját hálózatukon elhelyezett PROBE eszköz(ök) által begyűjtött teljes információhalmazt elérhetővé tesszük, részletes eseménynaplók, célpont toplisták formájában. Ennek segítségével elsődlegesen a begyűjtött adatok transzparenciáját

kívánjuk biztosítani, azonban a résztvevők számára hasznos eszközként is szolgálhat egy esetleges belső incidensfeltárási tevékenység során.

- A rendszerből származó adatokat a Hun-CERT saját incidenskezelési tevékenysége, valamint az ezzel kapcsolatos kutatási tevékenysége során felhasználhatja, azonban a tagok azonosítására alkalmas információkat (pl.: PROBE IP cím), az érintett felek eseti és explicit beleegyezése nélkül, nem adja tovább külső szereplők számára.



A PROBE eszköz hálózati viselkedése

A PROBE állomásokon jelen állapot szerint három alapvető szenzor funkció valósul meg. A Linux operációs rendszer tűzfal funkciója segítségével minden beérkező, egyébként kiszűrt, TCP vagy UDP csomag adatait naplózza, az eszköz ezen felül az alábbi, interaktív hálózati szolgáltatásokat nyújtja:

- SSH szenzor – a 22-es TCP porton porton érkező kérésekre valódi szerverként reagál. Egy egyszerűen kitalálható felhasználó/jelszó páros eltalálását követően valódinak látszó terminál környezetet biztosít, melyben valósnak látszó parancsok is kiadhatók. Az így elvégzett műveleteket a rendszer szintén naplózza.
- SMTP szenzor – a 25-ös TCP porton érkező kérésekre valódi mail szerverként reagál. Minden beérkező SMTP üzenetet átvesz, majd azonnal eldob. A beérkező adatokat (pl.: feladó, címzett, payload) naplózza.

- HTTP szenzor – a 80-as TCP porton érkező kérésekre valódi web szerverként reagál. Minden beérkező HTTP kérést sablon válasszal szolgál ki. A beérkező adatokat (pl.: URL, böngésző, javascript képességek) naplózza.

A fentiekben megadott szolgáltatásokon kívül a PROBE eszköz az alábbi, jelentősen korlátozott, önálló hálózati tevékenységet végzi. Kérjük, hogy ezeket a kommunikációs irányokat az eszköz elhelyezésénél tegyék lehetővé:

- PROBE központ (probe.cert.hu, jelenleg: 195.111.1.55) irányú OpenVPN kapcsolat fenntartása – a rendszer menedzsmentet, valamint a naplógyűjtést lehetővé tevő kapcsolatra a PROBE alapvető funkciójának megvalósításához van szükség. A VPN kapcsolat zárt és belső tűzfallal védett, az egyes PROBE eszközök, illetve a központ irányából csak szigorúan korlátozott szolgáltatások érhetők el.
- Nyilvános DNS szolgáltatás igénybevétele nyilvános resolvereken (pl.: 8.8.8.8, 8.8.4.4) keresztül – a rendszer indítása, illetve a manuális hálózati konfiguráció során a szonda a szolgáltatás igénybevételének segítségével csatlakozik a központi naplógyűjtő kiszolgálóra. Ezt követően privát DNS szolgáltatást használ a központi VPN kapcsolaton keresztül.
- Nyilvános NTP szolgáltatás igénybevétele nyilvános (ntp.org) időszolgáltatókon keresztül – a rendszer indítása során (permanens hardveres RTC hiányában) az időszinkronizálás a hálózati kapcsolódás előfeltétele.
- Helyi ARP kérések és válaszok küldése – a PROBE hálózati kapcsolatának működőképességének fenntartására használt szokványos helyi (LAN) protokoll.
- Helyi DHCP kérések és válaszok küldése – alapértelmezetten a PROBE eszközök hálózati konfigurációja DHCP protokoll segítségével történik. A PROBE eszközök manuális (statikus) IP konfigurációjára is lehetőség nyílik az alábbiakban ismertetett módon.
- Szabványos traceroute és ICMP echo request kérések küldése – alkalomszerűen, hálózati anomáliák felderítése érdekében, jellemzően a Hun-CERT üzemeltető munkatársai által manuálisan kiadott parancsok eredményeként.

Kérjük, hogy az eszközt lehetőleg olyan hálózati környezetbe helyezzék el, amely nem utal egyértelműen a felhasználás céljára és nem különbözteti meg feltűnően a PROBE eszközt egyéb hálózati eszközöktől. Ennek érdekében, kérjük, kerüljék a túlzottan egyértelmű PTR

rekordok, illetve az egyébként üres, más célra nem használt IP subnetek használatát. Kérjük, hogy egy C osztályú alhálózatra csak egy PROBE eszközt helyezzenek el.

Hálózati Konfiguráció (statikus IP cím)

A PROBE eszközök alapértelmezésben DHCP kérések segítségével szereznek hálózati konfigurációt. Amennyiben ez a tervezett célkörnyezetben nem megfelelő, lehetőség nyílik az állomások statikus IP konfigurációjára is.

Ennek érdekében az eszközre HDMI kijelzőt és USB billentyűzetet kell csatlakoztatni. Ezt követően a „netconf" felhasználónévvel és „netconf" jelszóval egy egyszerű és értelemszerűen működő konfigurációs script indul el, melynek segítségével a szükséges beállítások elvégezhetők, illetve ellenőrizhetők.

Megjegyzés: a „netconf" felhasználó természetesen csak fentiek szerinti fizikai hozzáférés esetén használható fel, az eszközhöz távoli adminisztrátori hozzáférést nem biztosít.

Nyilatkozatok

Az Hun-CERT nyilatkozik, hogy a jelen leírásban megadottaknak megfelelően, a PROBE eszközök viselkedési jellemzőin, valamint a begyűjtött adatok kezelési és felhasználási feltételein nem változtat a programban részt vevő támogatók (tagok) explicit beleegyezése nélkül. Kivételt képeznek ez alól az új passzív szenzor funkciók (tervben: NTP, DNS) bevezetése, illetve a kritikus biztonsági problémák javítása.

A Hun-CERT mindent megtesz annak érdekében, hogy a programban való részvétel a lehető legkisebb műszaki és jogi kockázattal járjon, azonban az elhelyezett eszközökkel, illetve a begyűjtött adatokkal kapcsolatba hozható közvetett, illetve közvetlen károkért anyagi felelősséget nem vállal.

A Hun-CERT fenntartja a jogot, hogy nem rendeltetésszerű felhasználás, visszaélési kísérlet, biztonsági incidens esetén az ezért felelős tagokat a programból kizárja.

A Hun-CERT fenntartja a jogot a programban résztvevő támogató tagok nevének és emblémájának nyilvános megjelenítésére a programmal kapcsolatos tájékoztató felületeken.

Csatlakozási feltételek

A PROBE programhoz bármely, fizikailag Magyarországon elhelyezkedő, nyilvános IP címen elérhető internetes szolgáltatási végpont tulajdonosa (magyar állampolgárságú

természetes személy vagy bejegyzett magyarországi telephellyel rendelkező jogi személy, cég, szervezet) csatlakozhat.

A csatlakozás feltétele, hogy a csatlakozó tag az általa elhelyezett PROBE eszköz rendeltetésszerű működését (tápellátás, Internet kapcsolat) díjmentesen és folyamatosan biztosítsa, valamint az eszköz számára biztosított fizikai hálózati csatlakozási pont és nyilvános IP cím felhasználási jogával rendelkezzen. A PROBE eszköz csak kizárólagosan számára dedikált, nyilvános IP címen helyezhető el.

A PROBE programhoz történő csatlakozás díjmentes. Az adatkezelési nyilatkozatban részletezettek szerint megosztott adatokhoz történő, tagi szintű hozzáférést az elhelyezett PROBE eszköz rendeltetésszerű működésének időtartamára biztosítjuk.

Kérjük, egy eszköz elhelyezésével Ön is támogassa a Hun-CERT PROBE programot! Támogatási szándékát az alábbi elérhetőségeinken jelezheti.

A programmal kapcsolatos csatlakozási és egyéb általános feltételek, nyilatkozatok mindenkor aktuális változata a program honlapján (https://www.cert.hu/probe) érhető el.

Kapcsolat

A PROBE eszköz jelenleg próbaüzemben működik. Csatlakozási szándék, valamint bármilyen kérdés, probléma, tapasztalat esetén az alábbi elérhetőségeken nyújtunk műszaki segítséget és tájékoztatást: cert@cert.hu illetve +36 1 279 6222