DEFENSE RESEARCH INSTITUTE OF MONGOLIA

Journal of Security and Defense Studies

Journal homepage:
https://mids.gov.mn/category/ayulgui_baidal-2/

ISSN: 2220-9115, E-ISSN: 2708-1230

Research Article

DOI: https://doi.org/10.65816/jsds.2026.02.018

Assessing the Attack Surface of Consumer iot Devices in Enterprise Networks: A Case Study of Smart tvs, IP Cameras, and Discovery Protocols

Unenbat Erdenesuvd[1], Dondogmegd Byambadorj[2], Batbayar Densmaa[3]

[1]PhD candidate in Defence and Security Studies, National Defense University of Mongolia; Head of the Department of Information Technology, Ider University, Ulaanbaatar, Mongolia, ORCID: 0009-0002-5135-3001

[2]Senior Lecturer, Ph.D., Department of Cybersecurity, Mongolian University of Science and Technology, Ulaanbaatar, Mongolia, ORCID: 0009-0006-6279-4573

[3]Associate Professor, Ph.D., Department of Cybersecurity, Mongolian University of Science and Technology, Ulaanbaatar, Mongolia, ORCID: 0000-0002-1016-9622

Received: 28 June 2026 *Revised: 02 July 2026*
Accepted: 22 July 2026 *Published online: 28 July 2026*

ABSTRACT

Consumer Internet of Things (IoT) devices such as smart televisions, IP cameras, wireless presentation devices, and connected printers increasingly operate on enterprise networks and introduce attack surfaces that may fall outside conventional endpoint controls. This paper assesses exposed services, discovery-protocol metadata, and local-network communication risks associated with consumer IoT devices through a pilot case study. Nmap/Zenmap was used for host and TCP service discovery, while Wireshark was used for packet-level inspection of ARP, SSDP/UPnP, WS-Discovery, and TCP traffic. A device documented as a Sony X75CH-series Android TV exposed TCP ports 8008, 8009, 8080, 8443, and 9000. SSDP M-SEARCH traffic was directed to 239.255.255.250:1900 to discover an InternetGatewayDevice:1 target. SSDP NOTIFY packets revealed device location, UPnP/DLNA server characteristics, and unique identifiers to the local network. The findings show that IoT attack-surface assessment should combine port exposure with service validation, discovery traffic, inter-segment reachability, firmware governance, and monitoring capability. A layered control set comprising IoT VLANs, ACL-based access control, multicast and discovery traffic restrictions, asset inventory, firmware lifecycle management, and SIEM-based monitoring is proposed.

Keywords: *Internet of Things, smart TV, IP camera, attack surface, Nmap, Zenmap, Wireshark, SSDP, UPnP, network segmentation.*

Байгууллагын сүлжээн дэх хэрэглээний зориулалттай IoT төхөөрөмжийн халдлагын гадаргууг үнэлэх нь: ухаалаг телевизор, IP камер ба төхөөрөмж илрүүлэх протоколын кейс судалгаа

Үнэнбат Эрдэнэсувд[1], Дондогмэгд Бямбадорж[2], Батбаяр Дэнсмаа[3]

[1]Үндэсний батлан хамгаалахын их сургуулийн Аюулгүй байдал судлалын докторант, Идэр их сургуулийн, Мэдээллийн технологийн тэнхимийн эрхлэгч, ORCID: 0009-0002-5135-3001

[2]Монгол Улсын Шинжлэх Ухаан технологийн их сургуулийн Кибер аюулгүй байдлын тэнхимийн ахлах багш, доктор (Ph.D), ORCID: 0009-0006-6279-4573

[3]Монгол Улсын Шинжлэх Ухаан технологийн их сургуулийн Кибер аюулгүй байдлын тэнхимийн дэд профессор, доктор(Ph.D) дэд профессор, ORCID: 0000-0002-1016-9622

ХУРААНГУЙ

Байгууллагын сүлжээнд ухаалаг телевизор, IP камер, утасгүй дэлгэц дамжуулах төхөөрөмж, сүлжээнд холбогдсон принтер зэрэг хэрэглээний зориулалттай зүйлсийн интернэт (IoT) төхөөрөмжийн хэрэглээ нэмэгдэхийн хэрээр уламжлалт төгсгөлийн төхөөрөмжийн хамгаалалтад үл хамрагдах шинэ халдлагын гадаргуу үүсэж байна. Энэхүү өгүүлэл нь байгууллагын орчинд холбогдсон хэрэглээний IoT төхөөрөмжөөс үүсэх ил гарсан сүлжээний үйлчилгээ, төхөөрөмж илрүүлэх протоколын мета өгөгдөл, локал сүлжээний харилцааны эрсдэлийг кейс судалгааны аргаар үнэлэв. Шинжилгээнд Nmap/Zenmap-аар хост ба нээлттэй TCP үйлчилгээ илрүүлэх, Wireshark-аар ARP, SSDP/UPnP, WS-Discovery болон TCP урсгалыг пакетын түвшинд задлан шинжлэх аргыг хослуулсан. Судалгааны кейсэд Sony X75CH-series Android TV гэж бариимтжуулсан төхөөрөмж дээр TCP 8008, 8009, 8080, 8443, 9000 портууд нээлттэй төлөвтэй илэрсэн. Мөн SSDP-ийн M-SEARCH хүсэлт 239.255.255.250:1900 multicast хаяг руу илгээгдэж, InternetGatewayDevice:1 төрлийн төхөөрөмжийн хайлт хийсэн нь тогтоогдсон. SSDP NOTIFY пакет нь төхөөрөмжийн байршил, UPnP/DLNA серверийн шинж, өвөрмөц таниг зэрэг мета өгөгдлийг локал сүлжээнд ил гаргах боломжтойг харуулав. Үр дүн нь IoT-ийн халдлагын гадаргууг зөвхөн нээлттэй портоор бус, үйлчилгээний бодит таних тэмдэг, discovery протокол, сегмент хоорондын хуртээмж, firmware-ийн удирдлага, мониторингийн чадавхаар хамтатган үнэлэх шаардлагатайг харуулж байна. Өгүүлэлд IoT VLAN, ACL-д суурилсан хандалтын хязгаарлалт, multicast/discovery урсгалын хяналт, төхөөрөмжийн бүртгэл, firmware-ийн амьдралын мөчлөгийн удирдлага, SIEM-д суурилсан мониторингийн багц арга хэмжээг санал болгосон.

Түлхүүр үгс: *зүйлсийн интернэт, ухаалаг телевизор, IP камер, халдлагын гадаргуу, Nmap, Zenmap, Wireshark, SSDP, UPnP, сүлжээний сегментчлэл.*

1. Удиртгал

Зүйлсийн интернэт нь хэрэглээний, байгууллагын болон сүлжээний дэд бүтцийн орчинд төхөөрөмж, программ хангамж, мэдрэгч, сүлжээний харилцан уялдааг өргөжүүлж байна. Ухаалаг телевизор, IP камер, ухаалаг самбар, сүлжээний хэвлэгч, хандалтын хяналтын төхөөрөмж зэрэг нь үйл ажиллагааны тав тухыг нэмэгдүүлдэг боловч байгууллагын дотоод сүлжээ рүү нэмэлт интерфейс, discovery үйлчилгээ, firmware-ийн хамаарал, өгөгдлийн урсгал, удирдлагын сувгийг оруулдаг. IoT төхөөрөмжийн кибер аюулгүй байдлын суурь чадавх нь төхөөрөмжийн таних, аюулгүй тохиргоо, өгөгдлийн хамгаалалт, логик хандалтын хяналт, программын шинэчлэлт, кибер төлөвийн хяналт зэрэгт тулгуурлах ёстой (Fagan et al. 2020, 2022; Rose et al. 2019).

Гэвч хэрэглээний зориулалтаар бүтээгдсэн олон IoT төхөөрөмж нь

байгууллагын endpoint management, patch management, EDR, төвлөрсөн лог менежментийн ердийн горимд бүрэн хамрагддаггүй. Иймээс халдлагын гадаргуу нь зөвхөн төхөөрөмжийн эмзэг байдлаас бус, тухайн төхөөрөмжийг хэн, аль VLAN-аас, ямар портоор, ямар discovery механизмаар олж харах боломжтой вэ гэдгээр тодорхойлогдоно. SSDP/UPnP болон WS-Discovery зэрэг протокол нь ашиглахад хялбар харилцан ажиллагааг дэмждэг ч төхөөрөмжийн төрөл, үйлчилгээ, байршлын URL, өвөрмөц таниг чийн талаарх мета өгөгдлийг сүлжээний орчинд ил гаргаж болно (Roman et al. 2013; UPnP Forum 2008; OASIS 2009).

Энэхүү судалгааны зорилго нь ухаалаг телевизор болон IP камертай холбоотой сүлжээний өгөгдлийн кейс дээр хэрэглээний IoT төхөөрөмж байгууллагын сүлжээний халдлагын гадаргууг хэрхэн тэлж байгааг тодорхойлох явдал юм. Иймд энэхүү судалгаа нь дараах гурван чиглэлд төвлөрөв. Үүнд: IoT төхөөрөмжүүд дээр ил гарч буй сүлжээний үйлчилгээг тодорхойлох; SSDP/UPnP болон бусад төхөөрөмж илрүүлэх протоколын урсгалаар ил болж буй төхөөрөмж, үйлчилгээний мета өгөгдлийг шинжлэх; илэрсэн эрсдэлийг бууруулах сүлжээний болон зохион байгуулалтын хяналтын арга хэмжээг тодорхойлох юм.

2. Судалгааны арга зүй

2.1. Судалгааны хүрээ ба өгөгдлийн эх үүсвэр

Судалгаанд диссертацийн ажлын хүрээнд баримтжуулсан хоёр төрлийн мэдээллийг ашиглав. Нэгдүгээрт, UB-19 нэртэй халдлагын өгөгдлийн сан болон байгууллагын сүлжээний пакетын шинжилгээнээс IP камер, SSDP/UPnP, ARP, WS-Discovery-тэй холбоотой урсгалын жишээг сонгов. Хоёрдугаарт, Zenmap ашиглан Sony X75CH-series Android TV (Android 5.0 гэж баримтжуулсан) төхөөрөмжийн нээлттэй TCP үйлчилгээний үр дүнг ашиглав. Судалгаанд ямар нэгэн эмзэг байдлыг ашиглах, нууц үг таах, үйлчилгээ тасалдуулах, firmware өөрчлөх, зөвшөөрөлгүй хандалт хийх үйлдэл гүйцэтгээгүй. Байгууллага, дотоод хост, MAC хаяг болон бусад таниг чийг өгүүлэлд нууцалсан. Эх өгөгдөл ба туршилтын дүрслэл нь диссертацийн хоёрдугаар бүлгийн сүлжээний шинжилгээний хэсэгт баримтжуулсан болно.

2.2. Шинжилгээний хэрэгсэл ба дараалал

Nmap/Zenmap-ыг хост илрүүлэх, TCP портын төлөв тогтоох, үйлчилгээний урьдчилсан таних тэмдэг авахад ашиглав. Nmap-ийн үйлчилгээний нэршил нь портын дугаар, хариу пакет, баннер болон fingerprint-ийн мэдээлэлд суурилсан урьдчилсан ангилал тул бодит үйлчилгээний баталгаажуулалт гэж үзэхгүй (Lyon 2009). Wireshark 4.4.5 ашиглан ARP, SSDP, UDP/1900, UDP/3702 болон сонгогдсон TCP урсгалыг пакетын түвшинд шалгав. Шинжилгээний логик дараалал нь (i) төхөөрөмж ба үйлчилгээ илрүүлэх, (ii) discovery урсгалыг ялгах, (iii) пакетын талбар болон мета өгөгдлийг задлах, (iv) эрсдэлийн нөлөөллийг ангилах, (v) хамгаалалтын хяналтыг тодорхойлох үе шаттай байв.

Хүснэгт 1. *IoT төхөөрөмжийн халдлагын гадаргууг үнэлэх шинжилгээний дараалал*

Үе шат	**Ашигласан хэрэгсэл / шүүлтүүр**	**Гаралт**
Хост ба порт илрүүлэх	Nmap/Zenmap	Ил хост, нээлттэй TCP порт, урьдчилсан service label

Discovery урсгалын шинжилгээ	Wireshark: ssdp, udp.port == 1900, udp.port == 3702	M-SEARCH, NOTIFY, WS-Discovery пакет, multicast чиглэл
Локал хаягжилт ба харилцаа	Wireshark: arp, tcp.port in {8008, 8009, 8080, 8443, 9000}	ARP broadcast, TCP session, SYN/ACK/RST дараалал
Эрсдэлийн үнэлгээ	Нотолгоонд суурилсан чанарын үнэлгээ	Ил байдал, discoverability, reachability, manageability, monitoring

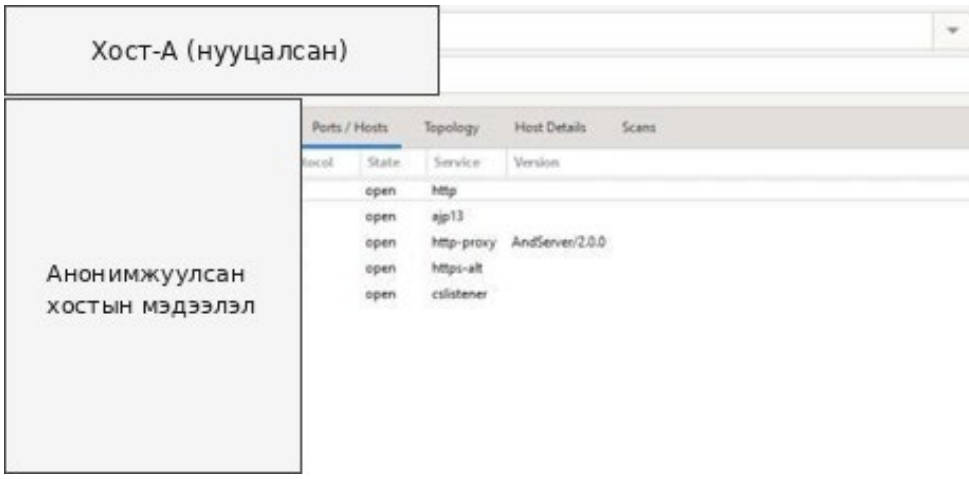
2.3. Эрсдэлийн үнэлгээний шалгуур

Халдлагын гадаргууг таван шалгууруар үнэлэв: (1) ил байдал - сүлжээнээс хүрч болох TCP/UDP үйлчилгээ; (2) илрэх боломж - SSDP, UPnP, WS-Discovery, ARP зэрэг механизмаар төхөөрөмж илрэх байдал; (3) хүрэх боломж - хэрэглэгч, зочин, серверийн сегментээс төхөөрөмжид хандах бодит боломж; (4) удирдлагын чадавх - төхөөрөмжийн бүртгэл, firmware, нэвтрэлт, тохиргооны хяналт; (5) мониторинг - сүлжээний лог, firewall, switch, DHCP, DNS, SIEM-ийн харагдац. Энэхүү үнэлгээ нь CVSS оноо биш; харин байгууллагын орчинд эрсдэлийн эх үүсвэрийг эрэмбэлэх чанарын хүрээ юм.

3. Үр дүн

3.1. Ухаалаг телевизорын ил гарсан TCP үйлчилгээ

Zenmap-ийн үр дүнгээр судалгаанд хамрагдсан ухаалаг телевизорын кейс хост дээр TCP 8008, 8009, 8080, 8443, 9000 портууд нээлттэй төлөвтэй илэрсэн. Зураг 1-д харагдах service label нь 8008, 8009 дээр “ajp13”, 8080 дээр “http-proxy / ANdServer/2.0.0”, 8443 дээр “https-alt”, 9000 дээр “cslistener” гэж урьдчилан ангилагдсан. Эдгээр label нь төхөөрөмжийн бодит үйлчилгээний эцсийн нотолгоо биш бөгөөд хариу баннер, TLS сертификат, протоколын handshake, үйлдвэрлэгчийн баримт бичиг, төхөөрөмжийн логийн уялдаа шаардлагатай. Иймээс энэ судалгаанд дээрх портуудыг батлагдсан эмзэг байдал гэж бус, хамгаалалтын хяналт шаарддаг ил гарсан сүлжээний интерфейс гэж үзэв.



Зураг 1. *Zenmap-аар илэрсэн кейс хостын нээлттэй TCP портууд (дотоод хостын мэдээллийг нууцалсан).*

Хүснэгт 2. *Кейс төхөөрөмж дээр илэрсэн TCP интерфейсийн нотолгоонд суурилсан тайлбар*

Порт	**Протокол**	**Zenmap-ийн урьдчилсан label**	**Эрсдэлийн тайлбар**	**Шаардлагатай баталгаажуулалт**
8008	TCP	ajp13	Ил гарсан application interface; бусад дотоод сегментээс хандах боломжийг шалгана.	Service banner, packet capture, ACL, үйлдвэрлэгчийн баримт
8009	TCP	ajp13	Ил гарсан application interface; хэрэглэгчийн workstation-той session ажиглагдсан.	Handshake, процессын лог, хэрэглээний зорилго
8080	TCP	http-proxy / ANdServer/2.0.0	HTTP-тэй холбоотой management/web interface байж болзошгүй.	HTTP header, authentication, TLS/ clear-text шалгалт
8443	TCP	https-alt	TLS-д суурилсан management интерфейс байж болзошгүй.	Сертификат, cipher suite, нэвтрэлт, exposure scope
9000	TCP	cslistener	Тодорхойгүй зориулалттай ил гарсан сервис.	Banner, service fingerprint, firmware болон vendor evidence

Төхөөрөмжийн нээлттэй портын тоо нь дангаараа аюулын хэмжүүр биш. Гэхдээ тухайн порт руу хэн хандаж болох, үйлчилгээ нь баталгаажуулалттай эсэх, TLS ашиглаж байгаа эсэх, firmware дэмжлэгтэй эсэх, байгууллагын активын бүртгэлд орсон эсэх нь нийлж эрсдэлийг тодорхойлно. Ялангуяа 9000 зэрэг тодорхойгүй үйлчилгээтэй портын бодит үүргийг баталгаажуулахгүйгээр “хортой” эсвэл “C2” гэж нэрлэх нь шинжлэх ухааны үндэслэлгүй юм.

3.2. SSDP/UPnP discovery урсгал ба мета өгөгдлийн ил байдал

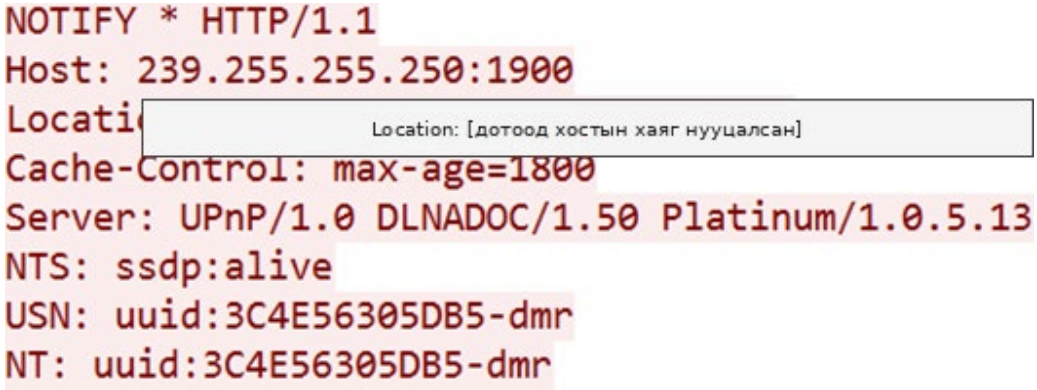
IP камертай холбоотой пакетын жишээнд SSDP M-SEARCH хүсэлт нь HOST: 239.255.255.250:1900 multicast хаяг руу илгээгдэж, ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1 зорилтот төрлөөр интернет гарцын төхөөрөмж хайсан байв. MAN: “ssdp:discover” нь хүсэлтийн шинжийг, MX: 1 нь хариу өгөх дээд хүлээлгийн хугацааг илэрхийлнэ. Энэ нь UPnP-ийн хэвийн discovery механизм боловч сегментчлэлгүй нөхцөлд төхөөрөмжийн байршил, боломжит gateway, үйлчилгээний бүтэц, цаашдын enumeration-д хэрэг болох мэдээллийг дотоод сүлжээнд ил гаргадаг (UPnP Forum 2008).

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1
MAN: "ssdp:discover"
MX: 1
```

Зураг 2. *239.255.255.250:1900 multicast хаяг руу илгээсэн SSDP M-SEARCH*

хүсэлт.

SSDP NOTIFY пакетын жишээнд төхөөрөмжийн Location талбар, UPnP/DLNA серверийн шинж, USN/UUID зэрэг өвөрмөц танигч дамжуулж байв. Тиймээс NOTIFY урсгал нь төхөөрөмжийг автоматаар илрүүлэхэд ашигтай боловч asset inventory-ийг зөвшөөрөлгүй цуглуулах, үйлдвэрлэгч ба программын хувилбарын талаарх fingerprint үүсгэх эрсдэлийг нэмэгдүүлж болно. Тухайн урсгал нь өөрөө халдлага биш боловч халдагч эсвэл халдварлагдсан endpoint-ийн discovery үе шатанд ашиглагдах мэдээллийн суурь болдог.



Зураг 3. *SSDP NOTIFY пакетэд агуулагдсан төхөөрөмжийн байршил, серверийн шинж ба өвөрмөц таниг чийн мета өгөгдөл (дотоод хостын хаягийг нууцалсан).*

3.3. ARP, WS-Discovery болон TCP урсгалын тайлбар

Пакетын өгөгдөлд ARP broadcast асуултууд, SSDP/UPnP урсгал, UDP 3702 портын WS-Discovery-тэй холбоотой тандах шинжтэй үйлдлүүд тэмдэглэгдсэн. WS-Discovery нь сүлжээний төхөөрөмж ба үйлчилгээ илрүүлэх зорилготой SOAP/XML-д суурилсан механизм бөгөөд IP камер, сүлжээний хэвлэгч, ухаалаг телевизор зэрэгт тохиолдож болно (OASIS 2009). Эдгээр протокол нь хэвийн ажлын урсгалын нэг хэсэг байж болох ч нэг сегментэд олон төрлийн төхөөрөмж байршсан үед IoT активыг хурдан тодорхойлох болон үйлчилгээний бүтэц гаргах боломжийг олгодог.

UB19 сангийн 2019 оноос хойш цуглуулсан судалгааны өгөгдөлд хостуудын хооронд TCP 8008, 8009 портоор ESTABLISHED төлөвтэй холболт үүссэн бөгөөд тухайн workstation-ийн PID нь chrome.exe процесстой уялдсан нь тэмдэглэгдсэн байна. Энэ нь browser-based casting, медиа удирдлага эсвэл веб суурьт харилцаатай нийцэж болох боловч пакетын хэсэгчилсэн мэдээллээр command-and-control урсгал, халдлага, эсвэл зөвшөөрөлгүй remote access гэдгийг батлах боломжгүй. Ийм дүгнэлт гаргахын тулд DNS/HTTP/TLS мета өгөгдөл, endpoint telemetry, хэрэглэгчийн үйлдэл, төхөөрөмжийн лог, хандалтын бодлогын нотолгоог хамтатган шалгах шаардлагатай.

Мөн ARP урсгалыг зөвхөн “ARP spoofing” гэж нэг мөр ангилах нь хангалтгүй. Нэг IP хаягт олон MAC хаяг хариулах, gateway-ийн MAC хаяг өөрчлөгдөх, unsolicited ARP reply, хаягжилтын тогтворгүй байдал, траффик чиглэл өөрчлөгдөх зэрэг дагалдах нотолгоо байж ARP spoofing-ийн дүгнэлтийг батална. Иймээс энэхүү өгүүлэлд ARP-ийн үр дүнг “IoT төхөөрөмж илрүүлэх болон локал сүлжээний

харагдцыг нэмэгдүүлж болох ARP-based activity” гэж болгоомжтой тайлбарлав.

3.4. Халдлагын гадаргуугийн нэгдсэн үнэлгээ

Хүснэгт 3. *IoT төхөөрөмжийн халдлагын гадаргуугийн нэгдсэн чанарын үнэлгээ*

Халдлагын гадаргуугийн бүрэлдэхүүн	**Нотолгоо**	**Эрсдэлийн түвшин**	**Тайлбар**
Ил гарсан TCP интерфейс	8008, 8009, 8080, 8443, 9000 нээлттэй	Өндөр	Зөвшөөрөлгүй сегментээс хүрэх боломж байвал lateral movement болон service enumeration эрсдэл нэмэгдэнэ.
SSDP M-SEARCH	239.255.255.250:1900, InternetGatewayDevice:1	Дунд	Gateway болон UPnP үйлчилгээний талаарх discovery мэдээлэл өгнө.
SSDP NOTIFY	Location, Server, USN/ UUID мета өгөгдөл	Дунд	Төхөөрөмжийн fingerprint болон asset enumeration-д ашиглагдах боломжтой.
WS-Discovery / UDP 3702	Төхөөрөмж, үйлчилгээ илрүүлэх урсгал	Дунд	IP камер, хэвлэгч, smart TV зэрэг активыг илрүүлэх механизм.
ARP-based activity	Broadcast ARP асуулт, локал хаягжилтын урсгал	Бага–дунд	Хэвийн протокол боловч гаж pattern байвал нэмэлт шалгалт шаардлагатай.
Төхөөрөмжийн удирдлага	Firmware, service identity, log visibility тодорхой бус	Өндөр	Нэгдсэн inventory ба patch governance байхгүй бол эрсдэл хуримтлагдана.

4. Хэлэлцүүлэг

Энэхүү кейсийн гол үр дүн нь хэрэглээний IoT төхөөрөмжийн халдлагын гадаргуу үйлчилгээний түвшин, discovery түвшин, сүлжээний хүртээмжийн түвшинд зэрэгцэн үүсдэгийг харуулсан явдал юм. Нэг талаас, олон TCP порт нээлттэй байгаа нь тухайн төхөөрөмж олон харилцан ажиллагааны интерфейстэйг илтгэнэ. Нөгөө талаас, SSDP/UPnP NOTIFY болон M-SEARCH урсгал нь орон нутгийн сүлжээнд төхөөрөмжийн талаарх мета өгөгдөл, байршил, үйлчилгээний шинжийг түгээж байна. Хэрэв хэрэглэгчийн сүлжээ, зочны сүлжээ, IoT сүлжээ, серверийн сүлжээ хооронд хэт өргөн харилцан хандалттай байвал discovery механизм нь тусгаарлагдсан байх ёстой төхөөрөмжүүдийн харагдцыг нэмэгдүүлнэ.

Нээлттэй портын утгыг тайлбарлахдаа болгоомжтой хандах шаардлагатай. Zenmap-ийн service label нь эхний шатны илрүүлэлт тул AJP, HTTP proxy, TLS эсвэл бусад үйлчилгээний бодит байдлыг дангаар нь тогтоохгүй. Түүнчлэн Chrome.exe-тай уялдсан TCP session нь casting эсвэл веб интерфейсийн хэвийн ажил байж болно. Өгүүллийн шинжлэх ухааны чанарыг хадгалахын тулд “нээлттэй порт”, “сэжигтэй discovery зан төлөв”, “анализ шаардсан үйлчилгээ” гэсэн баталгааны түвшний ойлголтыг “батлагдсан халдлага” гэсэн дүгнэлтээс салгаж авч үзэх нь зайлшгүй.

Илэрсэн нөхцөл нь байгууллага IoT төхөөрөмжийг энгийн хэрэглээний хэрэгсэл гэж биш, сүлжээнд холбогдсон удирдлагатай актив гэж үзэх шаардлагатайг харуулна. NIST-ийн IoT суурь чадавх болон zero-trust зарчим нь активын бүртгэл, хамгийн бага эрх, сүлжээний тусгаарлалт, тасралтгүй мониторинг, тохиргооны удирдлагаар энэ эрсдэлийг бууруулах боломжтойг онцолдог (Fagan et al. 2022, 2020; Cybersecurity and Infrastructure Security Agency 2023).

5. Эрсдэлийг бууруулах санал

Хүснэгт 4. *Байгууллагын IoT халдлагын гадаргууг бууруулах үе шаттай хяналтууд*

Чиглэл	Санал болгож буй хяналт	Хүлээгдэж буй үр нөлөө
Сегментчлэл	Smart TV, IP камер, принтер, мэдрэгчийг тусдаа IoT VLAN/ микросегментэд байрлуулах.	Хэрэглэгчийн endpoint-оос IoT руу чөлөөтэй lateral movement хийх боломжийг бууруулна.
Хандалтын хяналт	ACL/Firewall-аар зөвхөн зөвшөөрөгдсөн workstation, management host, шаардлагатай портод хандах эрх олгох.	8008, 8009, 8080, 8443, 9000 зэрэг интерфейсийн reachability-г хязгаарлана.
Discovery хяналт	VLAN хооронд SSDP/UPnP, multicast, UDP/1900, UDP/3702 урсгалыг default deny болгож, бизнесийн хэрэгцээгээр зөвшөөрөх.	Asset enumeration, gateway/ service discovery-ийн хүрээг багасгана.
Актив ба firmware	MAC, serial, model, firmware, эзэмшигч, байршил, ашиглалтын зорилгыг inventory-д бүртгэж, шинэчлэлтийг хянах.	Хуучирсан болон эзэнгүй төхөөрөмжөөс үүсэх эрсдэлийг бууруулна.
Мониторинг	Switch, firewall, DHCP, DNS, wireless controller, IDS/IPS, SIEM логийг IoT сегменттэй уялдуулах.	Гаж discovery, port scan, ARP anomaly, шинэ төхөөрөмж, гаднын хандалтыг илрүүлэх боломж нэмэгдэнэ.
Тохиргооны хамгаалалт	Анхдагч нууц үгийг солих, шаардлагагүй cloud/remote access, UPnP, guest pairing, debug service-ийг унтраах.	Ил гарсан interface болон зохисгүй remote management эрсдэл буурна.

6. Судалгааны хязгаарлалт

Нэгдүгээрт, судалгаа нь нэг ухаалаг телевизорын кейс, IP камертай холбоотой пакетын жишээ, discovery урсгалд тулгуурласан pilot судалгаа тул үр дүнг бүх үйлдвэрлэгч, бүх firmware, бүх байгууллагын сүлжээнд шууд ерөнхийлөхгүй. Хоёрдугаарт, Nmap/Zenmap-ийн service label нь үйлдвэрлэгчийн баталгаажуулалт, firmware-ийн задлан шинжилгээ, баннер, TLS сертификат, device log-оор баталгаажаагүй. Гуравдугаарт, судалгаанд эмзэг байдал ашиглах, нууц үг турших, firmware extraction, гадаад сүлжээний exposure шалгах, exploitability үнэлэх ажиллагаа ороогүй. Дөрөвдүгээрт, ажиглагдсан TCP, SSDP, ARP, WS-Discovery урсгал нь дангаараа халдлагын санаа зорилгыг нотлохгүй; үүнийг олон эх сурвалжийн telemetry-аар батлах шаардлагатай.

Цаашдын судалгаанд 10–20 IoT төхөөрөмжийг (smart TV, IP камер, router, access point, printer, wireless presentation system, access-control device, sensor) хамруулж, төхөөрөмжийн төрөл, firmware, ил порт, service fingerprint, encryption, authentication, VLAN, internet exposure, log availability гэсэн хувьсагчаар тоон харьцуулалт хийх нь зохистой. Үүний зэрэгцээ firmware-ийн дэмжлэг дууссан эсэх, CVE-тэй уялдсан эмзэг байдал, сегментчлэлийн өмнөх ба дараах attack-surface score-ийг тооцох нь эмпирик нотолгоог бэхжүүлнэ.

7. ДҮГНЭЛТ

Байгууллагын сүлжээнд байрлах хэрэглээний IoT төхөөрөмж нь нээлттэй TCP үйлчилгээ, discovery протоколын мета өгөгдөл, multicast урсгал, сегмент хоорондын хүртээмж, firmware болон мониторингийн сул удирдлагаар дамжин халдлагын гадаргууг тэлдэг. Кейс судалгаанд Sony X75CH-series Android TV гэж баримтжуулсан төхөөрөмж дээр TCP 8008, 8009, 8080, 8443, 9000 портууд нээлттэй илэрч, SSDP M-SEARCH нь 239.255.255.250:1900 multicast хаяг руу gateway discovery хийж, SSDP NOTIFY нь төхөөрөмжийн мета өгөгдлийг ил гаргаж байв. Эдгээр үр дүн нь IoT төхөөрөмжийг зөвхөн портын түвшинд биш, сервисийн бодит мөн чанар, discovery урсгал, network reachability, lifecycle governance, мониторингийн хамтатгасан хүрээнд үнэлэх шаардлагатайг нотолж байна.

Иймээс байгууллага IoT төхөөрөмжийг тусгай IoT сегментэд байрлуулах, зөвхөн хэрэгцээт хост ба портод ACL-ээр хандах, multicast/discovery урсгалыг VLAN хооронд хянах, актив ба firmware-ийн бүртгэл хөтлөх, гаж урсгалыг SIEM/IDS-ийн түвшинд илрүүлэх нэгдсэн хяналт хэрэгжүүлэх нь зүйтэй. Төхөөрөмжийн болон протоколын зан төлөвийг нотолгоонд суурилан тайлбарлах энэхүү арга нь төрийн болон хувийн хэвшлийн байгууллагын IoT эрсдэлийн үнэлгээнд ашиглах боломжтой.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. Cybersecurity and Infrastructure Security Agency. 2023. *Zero Trust Maturity Model, Version 2.0*. Cybersecurity and Infrastructure Security Agency.
2. Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. 2020. *IoT Device Cybersecurity Capability Core Baseline*. NISTIR 8259A. National Institute of Standards and Technology.
3. Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. 2022. *Profile of the IoT Core Baseline for Consumer IoT Products*. NISTIR 8425. National Institute of Standards and Technology.
4. Lyon, Gordon F. 2009. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project.
5. OASIS. 2009. *Web Services Dynamic Discovery (WS-Discovery) Version 1.1*. OASIS.
6. Roman, Rodrigo, Jianying Zhou, and Javier Lopez. 2013. “On the Features and Challenges of Security and Privacy in Distributed Internet of Things.” *Computer Networks* 57 (10): 2266–79. https://doi.org/10.1016/j.comnet.2012.12.018.

7. Rose, Karen, Scott Eldridge, and Lyman Chapin. 2019. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. NISTIR 8228. National Institute of Standards and Technology.
8. UPnP Forum. 2008. *UPnP Device Architecture, Version 1.0*. UPnP Forum.