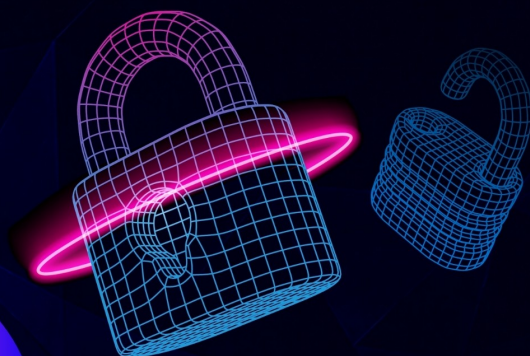




PUBLIC CSIRT/CC



CYBER READ

BADBOX BOTNET

Ухаалаг шинэчлэлийн далд өртөг

ХИЙМЭЛ ОЮУН БА КИБЕР АЮУЛГҮЙ БАЙДАЛ

С.БАДРАЛ

"Эгүнэ Оюун" ХХК-ийн үүсгэн
байгуулагч, гүйцэтгэх захирал



ЦАХИМААР
НЭН ТЭРГҮҮНД
ҮНДЭСНИЙ ХӨДӨЛГӨН

DARKWEB

орчинд алдагдсан монгол
нууц үгс



УХААЛАГ ШИНЭЧЛЭЛИЙН ДАЛД ӨРТӨГ

Энгийн зурагтыг ухаалаг болгох зориулалттай хямд **Android TV Box** төхөөрөмжүүд зах зээлд олноор худалдаалагддаг. Эдгээр төхөөрөмж нь шинэ зурагт авахаас хамаагүй хямд зардлаар төрөл бүрийн аппликэйшн ашиглах, кино болон бусад контент үзэх боломжийг санал болгодог.

Гэвч үл таних брэндийн хямд **TV Box** нь таны хувийн мэдээлэл алдагдах, гэрийн интернэт сүлжээ кибер халдлагад өртөх эрсдэлийг дагуулах эрсдэлтэй.



BadBox ботнетийг илрүүлсэн нь

Шинжээчид Badbox хорт программд шинжилгээ хийж, халдагчийн нууц шифрлэлтийг тайлан, ботнетийн дотоод холбоог илрүүлсэн. Үр дүнд олон мянган халдварласан TV Box-ууд удирдлагын команд болон хяналтын буюу Command-and-Control (C2) серверүүдтэй нууцаар холбогдож байжээ.

Халдвар зөвхөн телевизийн төхөөрөмжөөр хязгаарлагдаагүй. Windows үйлдлийн системтэй компьютеруудын дунд ч тархсан нь тогтоогдсон.

Дэлгэцийн цаана...

Кино үзэх зуур халдварласан төхөөрөмж “Трояны морь” мэт ажилласан:

01 Хуурамч зар сурталчилгаа ба хандалт

Үл үзэгдэх товшилтоор хандалт үүсгэж, зар сурталчилгааны орлогыг халдагчид завшсан.

02 Гэрийн интернет ашиглан халдлага үйлдсэн

Гэрийн IP хаягийг кибер гэмт хэргийн урсгалд ашиглан, үйлдлийг тухайн хаягнаас үйлдсэн мэт харагуулсан.

03 Хувийн мэдээлэл хулгайлах

Нэг удаагийн баталгаажуулах код (OTP) болон нэвтрэх нэр, нууц мэдээллийг хулгайлан, санхүүгийн хохирол учруулж байжээ.

Үйлдлийн системийн төөрөгдөл

Харагдах байдал
ANDROID 14



Бодит байдал
ANDROID 9

Android 14 гэж харагддаг ч үнэн хэрэгтээ 2018 оны Android 9 системтэй байжээ. Эмзэг байдал нь засагдаагүй систем нь гэрийн сүлжээг кибер халдлагын бай болгосон байна.

Монгол Улсын нөхцөл байдал

КХЗТНТ тус хортой программын хамгийн их хувийг эзэлж буй 5 домэйн дахь датанд дүн шинжилгээ хийв.



167

Мэдэгдсэн домэйн

Badbox хортой программтай холбоотой



5

Сонгосон домэйн

Хамгийн их холболт бүртгэгдсэн



3,070,478

хорт программ илэрсэн

Сонгогдсон 5 домэйн хаягт бүртгэгдсэн нийт холболтоос илэрсэн холболт



187,334

IP хаяг

Badbox хортой программтай холбоотой



2,391

Халдвар авсан төхөөрөмж

Хортой программын шинжилгээний үр дүн

КХЗТНТ-ийн Мэдээлэл дүн шинжилгээний газар

2026.08.20-ны байдлаар

УХААЛАГ ШИНЭЧЛЭЛИЙН ДАЛД ӨРТӨГ

Хямд TV Вох ашиглан зурагтаа ухаалаг болгох нь эдийн засгийн хувьд ашигтай мэт боловч таны хувийн мэдээлэл болон гэрийн интернэт сүлжээг эрсдэлд оруулж болзошгүй.

Иймд үл таних брэндийн хэт хямд төхөөрөмжөөс татгалзаж, албан ёсны баталгаатай газраас аюулгүй байдлын шинэчлэлийг тогтмол хийдэг найдвартай бүтээгдэхүүн сонгоорой.

Худалдан авахаасаа өмнө төхөөрөмжийн үйлдлийн системийн хувилбар болон үйлдвэрлэгчийн мэдээллийг заавал шалгаж байхыг анхаарна уу.



BadBox хорт программын халдвартай байж болзошгүй TV Вох төхөөрөмжийн загварууд

Таны төхөөрөмжийн загвар доорх жагсаалтын аль нэгтэй таарч байвал BadBox хорт программын халдвар авсан байх өндөр эрсдэлтэй:

X88-Pro-10	X96Q_PR01	TVBOX	GameBox
X96Q_Max_P	AV-M9	Smart	KM6
Q96L2	ADT-3	KM9PRO	X96Max_Plus2
X96Q2	OCBN	A15	TV007
X96mini	X96MATE_PLUS	Transpeed	Q9 Stick
S168	KM1	KM7	SP7731E
ums512_1h10_Natv	X96Q_PRO	iSinbox	H6
X96_S400	Projector_T6P	I96	X88
X96mini_RP	X96QPRO-TM	SMART_TV	X98K
TX3mini	sp7731e_1h10_native	Fujicom-SmartTV	TXCZ
HY-001	M8SPROW	MXQ9PRO	T95
MX10PRO	TV008	MBOX	T95Max
X96mini_Plus1	X96Mini_5G	X96Q	X12-Plus
LongTV_GN7501E	Q96MAX	isinbox	TV98
Xtv77	Orbsmart_TR43	Mbox	
NETBOX_B68	Z6	R11	

Windows үйлдлийн системтэй төхөөрөмжид:

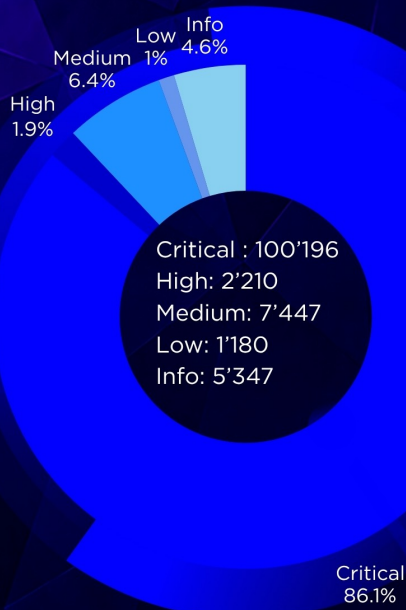
Windows үйлдлийн системтэй компьютерт дараах файлуудын аль нэг эсвэл хоёулаа системийн үйлчилгээ буюу service хэлбэрээр ажиллаж байвал тухайн компьютер халдвар авсан байх эрсдэлтэй:

AmanOnlineWT.exe	AmanUpdateLogLT.exe
------------------	---------------------

МОНГОЛ УЛСЫН КИБЕР ОРЧИН ДАХЬ 2026 АЮУЛ ЗАНАЛ НӨХЦӨЛ БАЙДЛЫН ТОЙМ МЭДЭЭ

2026.04.01 - 2026.08.31

ЭРСДЭЛИЙН ТҮВШИН



Тайлант хугацаанд 116,180 халдлага, зөрчил бүртгэгдсэний 100,196 нь Critical түвшнийх байна.

Critical түвшний эрсдэлийн 99,564 нь хорт програм (Malware), 632 нь Critical түвшний эмзэг байдал эзэлж байгаа бөгөөд эдгээрийг нэгтгэн Critical түвшний нийт дүнг тооцсон болно.

Critical = Critical Severity + Malware

Malware detected IP

99'564

IP хаягийн давхцлыг арилгасан

Critical Severity IP

632

IP хаягийн давхцлыг арилгасан

ХОРТ ПРОГРАММ

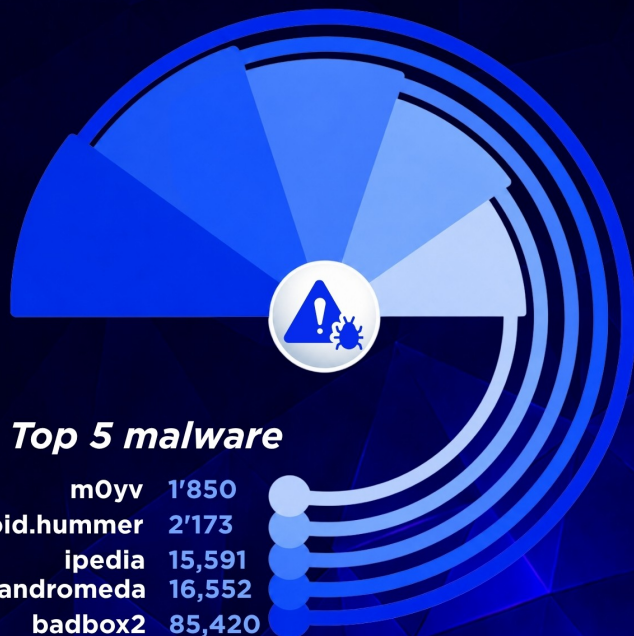
Malware Beacon

2'427'622

хорт программын гадагш
сигнал илгээсэн тоо
IP хаягийн давхцлыг арилгаагүй

Хорт программууд гадагш 2.4 сая гаруй удаа сигнал илгээсэн байна. Давхардсан IP хаягийг хасаж тооцоход badbox2 хамгийн олон хаягт бүртгэгдэж, бусад хорт программаас эрс өндөр үзүүлэлттэй гарсан.

Гадагш илгээсэн сигналын тоо нь халдварласан төхөөрөмжийн тоо гэсэн үг биш.



Top 5 malware

m0yv 1'850
android.hummer 2'173
ipedia 15,591
andromeda 16,552
badbox2 85,420

SCAN ХИЙГДСЭН ТӨХӨӨРӨМЖҮҮДИЙН АНГИЛАЛ

Үзүүлэлт бүрийн IP хаягийн давхцлын мэдээллийг тэмдэглэв

SCANNER

163'578

Эмзэг мэдээлэл хайсан үйлдлүүд

Давхцал арилгаагүй

EXPOSED

8'503

Ил харагдах шаардлагагүй төхөөрөмж

Давхцал арилгасан

POTENTIAL THREAT

3'526

Бусдад хохирол учруулж болохуйц

Давхцал арилгасан

KNOWN VULNERABILITY

2'460

Илэрсэн нийт эмзэг байдал

Давхцал арилгасан

VULNERABLE IoT

1'543

Smart төхөөрөмж, камер, router

Давхцал арилгасан

ATTACKER

559

Гадагш халдлага үйлдсэн

Давхцал арилгасан

BLACKLISTED IP

339

Олон улсад хаалт хийгдсэн IP

Давхцал арилгасан

END OF SUPPORT

250

Шинэчлэлт зогссон төхөөрөмж буюу программ хангамж

Давхцал арилгасан

MALWARE DISTRIBUTOR

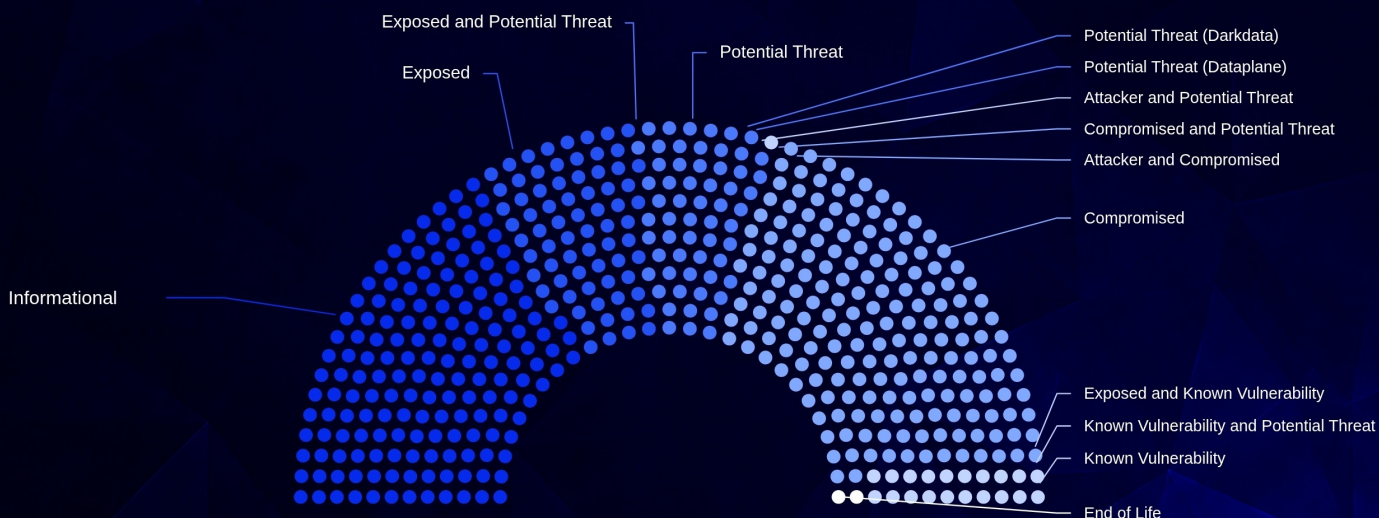
7

Хорт програм түгээгч хаяг

Давхцал арилгасан

НИЙТ БҮРТГЭГДСЭН ХАЛДЛАГА, ЗӨРЧЛИЙН ТОО

Халдлагад өртсөн ангилалд 99,414, интернэтэд нээлттэй ангилалд 8,503, мэдэгдэж буй эмзэг байдалтай ангилалд 2,460, үйлдвэрлэгчийн дэмжлэг, шинэчлэлт нь зогссон ангилалд 250 давхцалгүй IP хаяг бүртгэгдсэн.



Нийт мэдээллийн тоо / Давхцалгүй IP хаягийн тоо

Informational 1,666,447 / 10,680	Exposed 722,683 / 8,503	Exposed and Potential Threat 114,539 / 1,664	Potential Threat 381,714 / 3,526	Potential Threat (Darkdata) 43,715 / 1,027
Potential Threat (Dataplane) 63,586 / 189	Attacker and Potential Threat 983 / 559	Compromised and Potential Threat 4,573 / 195	Attacker and Compromised 18,642 / 962	Compromised 1,831,801 / 99,414
Exposed and Known Vulnerability 221 / 7	Known Vulnerability and Potential Threat 1,040 / 23	Known Vulnerability 178,172 / 2,460	End of Life 24,004 / 250	

- Эхний тоо нь нийт бүртгэгдсэн мэдээллийг,
- Хоёр дахь нь тухайн ангиллын давхцалгүй IP хаягийг илэрхийлнэ.

ЯРИЛЦЛАГЫН БУЛАН

Хиймэл оюун ба кибер аюулгүй байдал

Өгөгдлийн тусгаар тогтнол, эх хэл, технологийн бие даасан хөгжил болон аюулгүй байдлын тухай “Эгүнэ Оюун” ХХК-ийн үүсгэн байгуулагч, гүйцэтгэх захирал С.Бадралтай ярилцлаа.



SOP17-ын хүрээнд зохион байгуулагсан “Ногоон хиймэл оюун, дижитал шилжилт болон шинжлэх ухаан” арга хэмжээнд ямар сэдвээр оролцсон бэ?

“Эгүнэ Оюун” ХХК 2018 оноос хойш үндэсний их хэлний загвар (LLM) болон хиймэл оюуны суурь загвар хөгжүүлж ирсэн туршлагатай. Илтгэлийн үеэр Монгол Улсын нөхцөл, хэл, хэрэглэгчдийн бодит хэрэгцээнд нийцсэн үндэсний суурь загварыг хэрхэн хөгжүүлж буй талаар танилцуулж, өөрсдийн хуримтлуулсан туршлага, технологио бие даасан хиймэл оюун хөгжүүлэх боломж хязгаарлагдмал улс орнуудад түгээн дэлгэрүүлэх, цаашлаад экспортлох боломжтойг онцолсон юм.

Өнөөдөр хиймэл оюуны загварыг улам томруулахын хэрээр дата төв, цахилгаан эрчим хүч, ус, тооцоолох хүчин чадал зэрэг асар их нөөц шаардагдаж байна. Гэвч аливаа асуудлыг заавал хамгийн том загвараар шийдвэрлэх шаардлагагүй. Харин тухайн нөхцөл, хэрэгцээнд тохирсон оновчтой, үр ашигтай загвар хөгжүүлэхгүй бол технологийн хөгжил дэлхийн нөөцийг шавхаж, “ногоон дэлхийгээ хар дэлхий болгох” эрсдэлтэйг илтгэлээр анхааруулсан.

Манай компанийн зүгээс Монгол Улсын бодит нөөц боломж, хөрөнгө оруулалтын чадавхад тулгуурлан хиймэл оюуны суурь загвар хөгжүүлэх боломжийг танилцуулсан. Илтгэлийн гол санаа нь хиймэл оюуныг улам томруулах бус, илүү ухаалаг, хүртээмжтэй, үр ашигтай, байгаль орчинд ээлтэй байдлаар хөгжүүлэх цаг ирснийг олон улсад хүргэх нь гол зорилго байлаа.



С.БАДРАЛ

“Эгүнэ Оюун” ХХК-ийн үүсгэн байгуулагч, гүйцэтгэх захирал



Үндэсний хиймэл оюун бол биелэшгүй зорилго биш, бодитоор хэрэгжүүлэх боломжтой хөгжлийн зам юм. Монгол хэл, соёл, үнэт зүйлд суурилсан AI нь эмзэг мэдээллийг улсын хил дотор найдвартай хадгалж, төр, хувийн хэвшлийн дижитал хараат бус байдлыг бэхжүүлнэ. Монгол Улс өөрийн суурь AI загварыг хөгжүүлснээр хиймэл оюуны ирээдүйгээ өөрсдөө тодорхойлох боломжтой болж байна.

01 Үндэсний хиймэл оюун хөгжүүлэхэд “өгөгдлийн тусгаар тогтнол” яагаад чухал вэ? Egune AI эмзэг мэдээллийг хэрхэн хамгаалж байна вэ?

Ямар ч улс орон цахилгаан, ус, зам тээвэр зэрэг стратегийн дэд бүтцээ бусдаас бүрэн хамааралтай байлгахыг хүсдэггүй. Үүнтэй адил хиймэл оюун өнөө цагийн “дижитал дэд бүтэц” болж байна. Тиймээс Монгол Улс өөрийн хэл, соёл, хууль эрх зүйн орчинд нийцсэн үндэсний хиймэл оюунтай байх шаардлагатай.

Үүний гол үндэслэл нь мэдээллийн аюулгүй байдал, өгөгдлийн тусгаар тогтнол юм. Иргэн, төр, байгууллагын өгөгдлийг хамгаалж, Хүний хувийн мэдээлэл хамгаалах тухай болон Кибер аюулгүй байдлын тухай хуулийг бодитоор хэрэгжүүлэхийн тулд гаднын системээс хамаардаггүй технологийн орчин хэрэгтэй. Egune AI нь өгөгдлийг Монгол Улсад хадгалж, боловсруулах боломжтой үндэсний суурь загвар хөгжүүлэхээр ажиллаж байна.

Үндэсний хиймэл оюун нь монгол хэл, өв соёлоо хамгаалах ач холбогдолтой. “Эгүнэ” ХХК өмнө нь BolorSpell программыг хөгжүүлсэн туршлагадаа тулгуурлан монгол хэлээр зөв ярьж, оновчтой найруулдаг, эх хэлний утга, аялгууг хадгалсан хиймэл оюуныг бүтээхийг зорьж байна.

Мөн гадаадын үйлчилгээнд төлж буй төлбөр, дамжуулж буй өгөгдлөө дотооддоо үлдээж, үндэсний оюуны өмч, технологийн экспортыг хөгжүүлэх нь эдийн засгийн хувьд чухал. “Эгүнэ”-г бид хувь хүний өмч бус, Монголын ирээдүйд үлдэх оюуны өв гэж хардаг.

ЯРИЛЦЛАГЫН БУЛАН

Хиймэл оюун ба кибер аюулгүй байдал



02 Хиймэл оюун кибер халдлагад өртөх эрсдэлтэй өнөө үед “Эгүнэ” ХХК байгууллагын мэдээлэл, дотоод систем, хөгжүүлэлтийн орчныхоо аюулгүй байдлыг хэрхэн ханган ажиллаж байна вэ?

Хиймэл оюуны загвар төдийгүй бүх дижитал систем кибер халдлагад өртөх эрсдэлтэй. Ямар ч технологи, стандарт системийг 100 хувь хамгаалж чадахгүй учраас аюулгүй байдлыг зөвхөн мэргэжилтний үүрэг бус, байгууллагын нийт ажилтны оролцоотой цогц үйл явц гэж үздэг.

Манай байгууллага мэдээллийн аюулгүй байдлын ISO/IEC 27001 стандартыг дотоод үйл ажиллагаандаа хэрэгжүүлэхэд анхаарч, хүн, үйл ажиллагааны процесс, технологийн түвшинд эрсдэлийг удирдан ажилладаг. Үйлчлэгчээс эхлээд хөгжүүлэгч хүртэл ажилтан бүр аюулгүй байдлын тогтолцооны нэг хэсэг юм.

Технологийн хувьд дотоод харилцаандаа өөрсдийн хөгжүүлсэн “Bolorchat”-ыг ашигладаг. Мөн байгууллагын автоматжуулалт, мэдээллийн систем болон шаардлагатай бусад программын шийдлээ дотооддоо хөгжүүлж, хаалттай орчинд ажиллуулдаг.

Egune AI-ийн загваруудад гаднын хиймэл оюуны загвар ашигладаггүй бөгөөд өөрсдийн бүтээсэн загвар, системд тулгуурладаг. Ийнхүү өгөгдөл, систем, хөгжүүлэлтийн орчноо дотооддоо хянах нь prompt injection, өгөгдөл алдагдах, зөвшөөрөлгүй хандалт болон загварт чиглэсэн халдлагын эрсдэлийг бууруулах үндсэн хамгаалалт болдог.

“Эгүнэ”-г Монголын ирээдүйд үлдэх оюуны өв гэж хардаг.

03 Үндэсний хиймэл оюун Монгол Улсын мэдээлэл, кибер аюулгүй байдлын орчныг бэхжүүлэхэд хувь нэмрээ оруулж чадах уу? Энэ чиглэлд Egune AI ямар боломжтой вэ?

Үндэсний хиймэл оюуны гол зорилго нь зөвхөн техникийн хамгаалалт бус, deepfake, худал мэдээлэл, нийгмийн инженерчлэл зэрэг сэтгэл зүй, мэдээллийн орчинд чиглэсэн аюулаас хамгаалах чадавхыг нэмэгдүүлэхэд чухал үүрэгтэй гэж хардаг.

Монголын нийгэм Facebook платформоос мэдээллээ түлхүү авдаг тул худал, төөрөгдүүлсэн мэдээлэл богино хугацаанд өргөн тархах эрсдэлтэй. Egune AI нь ийм мэдээллийг илрүүлэх, ангилах, эх сурвалжийг нягтлахад дэмжлэг үзүүлж, иргэдийг мэдээлэлд шүүлтүүртэй хандахад туслах боломжтой.

Мөн төрийн үйл ажиллагаанд хиймэл оюуныг нэвтрүүлснээр хүний оролцоог бууруулж, ил тод, шударга шийдвэр гаргалтыг дэмжинэ. Тухайлбал, “Эрдэнэт үйлдвэр” ТӨҮГ тендерийн сонгон шалгаруулалтад хиймэл оюун ашиглаж байгаа нь сайн жишиг юм. Монгол Улсын дээд шүүхэд Монгол Улсын хууль тогтоомжид тулгуурласан үндэсний их хэлний загвар (LLM) хөгжүүлэхэд Egune AI-ын жижиг загваруудыг ашиглан хамтран ажиллаж байна.

Цаашид цахилгаан эрчим хүч, дата төв, тооцоолох хүчин чадлыг бүрдүүлж чадвал үндэсний хиймэл оюуныг бүх салбарт нэвтрүүлэх боломжтой. Ингэснээр стратегийн болон эмзэг мэдээллээ дотооддоо хадгалж, гаднын систем, технологиос хамаарах хамаарлыг бууруулан, технологийн бие даасан байдал цаашлаад үндэсний аюулгүй байдлаа бэхжүүлнэ гэж харан, Үндэсний хиймэл оюуныг хөгжүүлж байна.

ЦАХИМААР НЭН ТЭРГҮҮНД



Монгол Улсын Засгийн газрын 108 дугаар тогтоолоор баталсан “Цахимаар нэн тэргүүнд” бодлогын зөвлөмжийн хүрээнд төрийн үйлчилгээг илүү шуурхай, хүртээмжтэй, иргэн төвтэй болгох зорилго бүхий “Цахимаар нэн тэргүүнд” үндэсний хөдөлгөөнийг ЦХИХХЯ санаачлан хэрэгжүүлж байна.

2026.03.25-26

Дорноговь аймаг

“Цахим Дорноговь” өдөрлөгийг ЦХИХХЯ, харьяа байгууллагууд болон төр, хувийн хэвшлийн түншлэлийн хүрээнд хамтран зохион байгуулж, хиймэл оюун, кибер аюулгүй байдал, төрийн цахим үйлчилгээ зэрэг сэдвүүдээр иргэдэд мэдлэг, ойлголт түгээж ажиллалаа.



Нийт 1340 хүүхэд, залуус, ахмад настан, хөгжлийн бэрхшээлтэй иргэд, хугацаат цэргийн албан хаагчид, харилцаа холбоо, мэдээллийн технологийн ажилчид, төрийн албан хаагчдад:

- “Хиймэл оюунд суурилсан халдлагууд”,
- “Цахим орчны сэтгэл зүй ба нийгмийн эрсдэл”,
- “Фишинг залилан ба хиймэл оюунд суурилсан халдлага”,
- “Халдлага, зөрчил илэрсэн үед авах хариу арга хэмжээ”
- “Кибер аюулгүй байдлын өнөөгийн нөхцөл байдал ба бодит аюул” сургалтуудыг амжилттай зохион байгууллаа.

2026.05.27-28

Сонгинохайрхан дүүрэг



“Цахим Сонгинохайрхан” өдөрлөгийг 4 бүсэд нийт 5000 хүүхэд, залуус, ахмад настан, хөгжлийн бэрхшээлтэй иргэд, хугацаат цэргийн албан хаагчид, төрийн албан хаагчид, цагдаагийн алба хаагчдад:

- “Кибер аюулгүй байдал: Иргэн бүрийн мэдэх ёстой 5 зүйл”,
- “Хиймэл оюунд суурилсан халдлагууд”,
- “Цахим орчны сэтгэл зүй ба нийгмийн эрсдэл”,
- “Фишинг залилан” сургалтуудыг амжилттай зохион байгууллаа.

ҮНДЭСНИЙ ХӨДӨЛГӨӨН

Монгол Улсын Ерөнхий сайдын 2026 оны 99 дүгээр захирамжаар шүүх, хууль сахиулах байгууллагуудын уялдаа холбоог сайжруулах, хэрэг хянан шийдвэрлэх ажиллагааг цахим хэлбэрт шилжүүлэхтэй холбоотой нөхцөл байдлыг үнэлэх Ажлын хэсэг байгуулагдсан.

2026.06.09

Сонгинохайрхан дүүрэг

Энэ хүрээнд Цахим хөгжил, инновац, харилцаа холбооны яам, Кибер аюулгүй байдлын зөвлөл, Цагдаагийн ерөнхий газар хамтран **“Цагдаагийн алба хаагчдыг кибер аюулгүй байдлын чиглэлээр чадавхжуулах хөтөлбөр”**-ийг амжилттай хэрэгжүүллээ.

Хөтөлбөрийн хүрээнд Сонгинохайрхан дүүргийн Цагдаагийн газрын 203 алба хаагчийг хамруулсан сургалтыг зохион байгуулж, кибер орчинд үйлдэгдэж буй гэмт хэрэг, цахим залилангийн өнөөгийн нөхцөл байдал, түүнээс урьдчилан сэргийлэх арга зам, мөрдөн шалгах ажиллагаанд ашиглагдах арга зүй, практик ур чадварын талаар мэдлэг, мэдээлэл олголоо.

Тус сургалт нь цагдаагийн алба хаагчдын кибер гэмт хэрэгтэй тэмцэх мэдлэг, ур чадварыг нэмэгдүүлэх, цахим орчин дахь эрсдэлийг бууруулах, иргэдийг гэмт хэргээс урьдчилан сэргийлэх үйл ажиллагааны үр нөлөөг дээшлүүлэхэд чухал ач холбогдолтой юм.

2026.06.15

Баянгол дүүрэг

Баянгол дүүргийн Цагдаагийн газрын 188 алба хаагчдыг кибер орчинд үйлдэгдэж буй гэмт хэргээс урьдчилан сэргийлэх чиглэлийн сургалтад хамрууллаа.

Мөн 2026 оны 6 дугаар сарын 2-3-ны өдрүүдэд зохион байгуулагдсан “ЦЕГ-ын мөрдөгчдийн цахим залилан болон кибер гэмт хэрэгтэй тэмцэх чиглэлийн мэргэжлийн ур чадварыг дээшлүүлэх хөтөлбөр”-ийг амжилттай дүүргэсэн Сонгинохайрхан болон Баянгол дүүргийн Цагдаагийн газрын цахим гэмт хэрэгтэй тэмцэх чиглэлийн мөрдөгчдөд гэрчилгээ гардууллаа.



ҮЙЛ ЯВДЛЫН ТОЙМ



КИБЕР АЮУЛГҮЙ БАЙДЛЫН ТЭМЦЭЭНД ТЭРГҮҮН БАЙР ЭЗЭЛЛЭЭ



ФИНТЕК БА КИБЕР АЮУЛГҮЙ БАЙДАЛ ХАМТАРСАН УУЛЗАЛТ

05.13

Security Transformation Forum-ийн “Human + AI | Redefining Cybersecurity” сэдвийн хүрээнд төрийн болон хувийн хэвшлийн байгууллагуудын дунд зохион байгуулсан “Ultimate Fabric Challenge 2026” кибер аюулгүй байдлын тэмцээнд амжилттай оролцлоо.

Тэмцээнд Кибер халдлагад хариу үзүүлэх газрын **шинжээч Э.Ганбаяр** тэргүүн байр, **шинжээч Б.Билгүүндай** гутгаар байр эзэлж, мэргэжлийн өндөр ур чадвараа батлан харуулав.

Бодит нөхцөлд тулгуурласан тус тэмцээнээр оролцогчдын кибер аюулгүй байдлын мэдлэг, техникийн ур чадвар, халдлагыг илрүүлэх, шинжлэх болон шуурхай хариу арга хэмжээ авах чадавхыг сорьсноороо онцлог байв.

05.19

Цахим хөгжил, инновац, харилцаа холбооны яам, Цагдаагийн ерөнхий газар, Харилцаа холбооны зохицуулах хороо, Монголын банкны холбоо, ЖАЙКА болон “Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ хамтран

“Цахим залилангаас сэргийлэх”

үндэсний аяныг нэг сарын хугацаанд амжилттай зохион байгууллаа.

Цахим залилангийн түгээмэл арга, хэлбэрийг таниулах, урьдчилан сэргийлэх зөвлөмж, сэрэмжлүүлгийг тогтмол хүргэх, иргэдийн цахим аюулгүй байдлын мэдлэгийг дээшлүүлэх чиглэлээр нийт 25 арга хэмжээг орон даяар хэрэгжүүллээ.

Мөн иргэдэд нууц үг, банкны болон хувийн мэдээллээ бусдад дамжуулахгүй байх, цахим эрсдэлийг таньж, өөрийгөө болон гэр бүлээ хамгаалах зөв дадлыг хэвшүүлэхэд чиглэсэн.

06.03

“Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ Монголын **Финтекийн холбоо болон финтекийн салбарын 28 байгууллагын төлөөлөлтэй уулзалт** зохион байгууллаа.

Уулзалтаар кибер халдлага, зөрчлийн өнөөгийн нөхцөл байдал, хууль эрх зүйн орчны хэрэгжилт, болзошгүй эрсдэлээс урьдчилан сэргийлэх арга хэмжээний талаар мэдээлэл хүргэв.

Мөн салбар хоорондын хамтын ажиллагааг бэхжүүлэх, мэдээлэл солилцоог сайжруулах болон цаашид хамтран хэрэгжүүлэх ажлын чиглэлүүдийн талаар санал солилцлоо.

ҮЙЛ ЯВДЛЫН ТОЙМ



ОНЦ ЧУХАЛ МЭДЭЭЛЛИЙН ДЭД БҮТЦИЙН КИБЕР АЮУЛГҮЙ БАЙДЛЫН СУРГАЛТ

06.12

Цахим хөгжил, инновац, харилцаа холбооны яамнаас Японы Олон улсын хамтын ажиллагааны байгууллага (ЖАЙКА)-ын “Кибер аюулгүй байдлын хүний нөөцийг хөгжүүлэх төсөл”-ийн нэгжтэй хамтран “Онц чухал мэдээллийн дэд бүтцийн кибер аюулгүй байдал” сургалтыг зохион байгууллаа.

Тус сургалтад төрийн болон хувийн хэвшлийн 92 байгууллагын 130, орон нутгийн 20 албан хаагч хамрагдсан нь энэхүү арга хэмжээний ач холбогдол, цар хүрээг илтгэж байлаа.

Сургалтын гол зорилго нь онц чухал мэдээллийн дэд бүтцийн кибер аюулгүй байдлын чиглэлээрх Ази, Номхон далайн бүсийн зарим орны хууль эрх зүйн зохицуулалт, сайн туршлагыг танилцуулах, улмаар кибер халдлагад хариу үзүүлэх төлөвлөгөө боловсруулах дадлага ажлаар дамжуулан оролцогчдын мэдлэг, ур чадварыг нэмэгдүүлэхэд чиглэсэн юм.



ХАРИЛЦАА ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН САЛБАРЫН ҮҮСЭЖ ХӨГЖСӨНИЙ 105 ЖИЛИЙН ОЙ

07.31

Монгол Улсад орчин цагийн харилцаа холбоо, мэдээллийн технологийн салбар үүсэж хөгжсөний 105 жилийн ой тохиолоо.

Энэ хүрээнд салбарын төр, хувийн хэвшлийн байгууллагууд хамтран Төрийн ордны Их танхимд арга хэмжээ зохион байгууллаа.

Цахим хөгжил, инновац, харилцаа холбооны сайд Ч.Номин илтгэл тавьж, салбарын бодлогын тэргүүлэх чиглэлүүдээ танилцуулсан бөгөөд “Цахим шилжилтийг эрчимжүүлж, салбарын бодлого, үйл ажиллагааг иргэн, бизнесийн хэрэгцээнд нийцүүлэх, төрийн үйлчилгээг илүү хялбар, шуурхай, чирэгдэлгүй хүргэх, хууль эрх зүйн орчныг шинэчлэх, мэдээллийн аюулгүй байдлыг бэхжүүлэх, бүх нийтийн цахим ур чадварыг дээшлүүлэх, төр хувийн хэвшлийн түншлэл болон гадаад хамтын ажиллагааг өргөжүүлэхээр ажиллаж байгаа”-г онцлов.



ЦӨЛЖИЛТЭЙ ТЭМЦЭХ ТУХАЙ НҮБ-ЫН КОНВЕНЦЫН ТАЛУУДЫН 17 ДУГААР БАГА ХУРАЛ

08.18

Цахим хөгжил, инновац, харилцаа холбооны яам болон харьяа, салбар байгууллагууд Цөлжилттэй тэмцэх тухай НҮБ-ын конвенцын Талуудын 17 дугаар бага хурлын хүрээнд “**Ногоон хиймэл оюун, дижитал шилжилт болон шинжлэх ухаан**” сэдэвт арга хэмжээг зохион байгуулж, Монгол Улсын технологи, эрдэм шинжилгээ, хувийн хэвшлийн төлөөллүүд хиймэл оюуны шинэлэг шийдэл, туршлагаа хуваалцлаа.

Хиймэл оюун, дижитал шилжилтийн хэрэглээ өсөн нэмэгдэхийн хэрээр кибер болон мэдээллийн аюулгүй байдал улам чухал болж байгааг оролцогчид онцоллоо.

Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв нь чиг үүргийнхээ хүрээнд тус хурлын техник, технологи, зохион байгуулалт болон мэдээллийн аюулгүй байдлын хүрээнд дэмжлэг үзүүлэн хамтран ажиллалаа.

DARKWEB ОРЧИНД АЛДАГДСАН МОНГОЛ НУУЦ ҮГС

Г.Батмөнх
Мэдээлэл дүн шинжилгээний
газрын ахлах судлаач

Б.Ану-Үжин
Мэдээлэл дүн шинжилгээний газрын
халдлага зөрчлийн тайлан мэдээ
хариуцсан мэргэжилтэн

Энэхүү судалгаа нь **DarkWeb** орчинд хууль бусаар тархсан, Монгол хэрэглэгчидтэй хамаарал бүхий нууц үгсийн бүтэц, давтамж, хэвшмэл загвар болон аюулгүй байдлын эрсдэлийн түвшинд дүн шинжилгээ хийсэн болно.

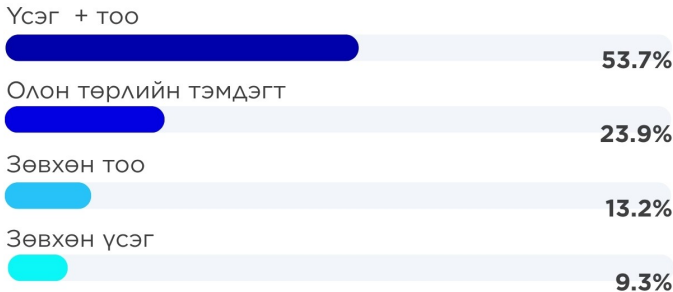
Судалгааны хамрах хүрээ

Судалгаанд нийт **4,254 өгөгдөл** цуглуулсан. Давхардсан, дутуу болон шинжилгээнд ашиглах боломжгүй мэдээллийг хасан **4,119 нууц үгийг** эцсийн түүвэрт хамруулсан.

Хувь хүнийг шууд таних боломжтой мэдээллийг бүрэн хасаж, зөвхөн нууц үгийн урт, тэмдэгтийн бүрдэл, давтамж, хэвшмэл бүтэц болон энтропид суурилсан эрсдэлийг үнэлэв.

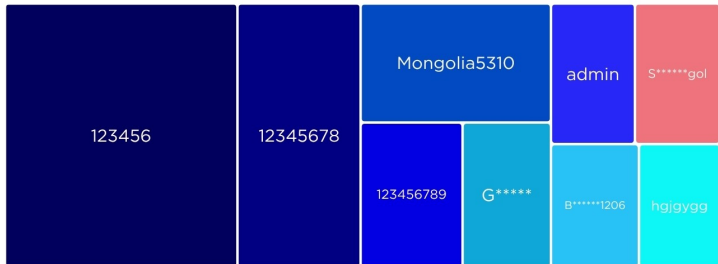
Нууц үгийн бүтэц

Судалгаанд хамрагдсан нууц үгийн тархалтаас үзэхэд **8 тэмдэгтийн урттай нь 810 тохиолдол** байсан нь хамгийн түгээмэл байв.



Урт нууц үг хэрэглэсэн ч бүтэц нь энгийн байх тохиолдол түгээмэл байгааг харуулж байна.

Давтамж ба хэвшмэл байдал



Хамгийн их давтагдсан нууц үг:

- “123456” - 62 удаа,
- “12345678” - 33 удаа бүртгэгдсэн.

Нууц үгсийн

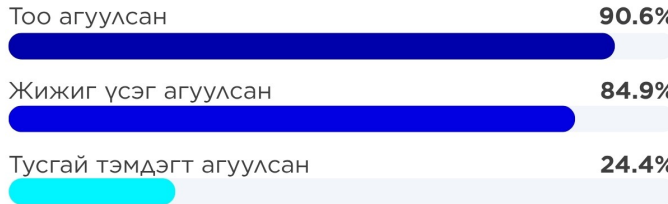
- 11.48% нь “123”, “abc” зэрэг дараалал,
- 4.49% нь огнооны мэдээлэл агуулжээ.

Өөрөөр хэлбэл, нийт нууц үгийн ойролцоогоор 16% нь таамаглахад хялбар хэвшмэл бүтэцтэй байна.

Тэмдэгтийн хэрэглээ

Хэрэглэгчид санахад хялбар, энгийн бүтэцтэй хувилбарыг түлхүү сонгодгийг илтгэнэ.

Тусгай тэмдэгт оруулах нь дангаараа бат бөх нууц үг бий болгохгүй ч нийтлэг дараалал болон хувийн мэдээлэлтэй хослоогүй үед таамаглахад хэцүү болгоно.



Эрсдэлийн үнэлгээ

34.5% дунд, өндөр, нэн өндөр эрсдэлтэй

Энтропид суурилсан үнэлгээгээр нууц үгийн 65.5% нь эрсдэл багатай ангилалд орсон.

Гэсэн хэдий ч үлдсэн хэсэг нь дунд, өндөр, нэн өндөр эрсдэлтэй байсан нь хэрэглэгч, байгууллагын түвшинд нууц үгийн хамгаалалтаа сайжруулах шаардлагатайг харуулж байна.

Судлаачийн дүгнэлт

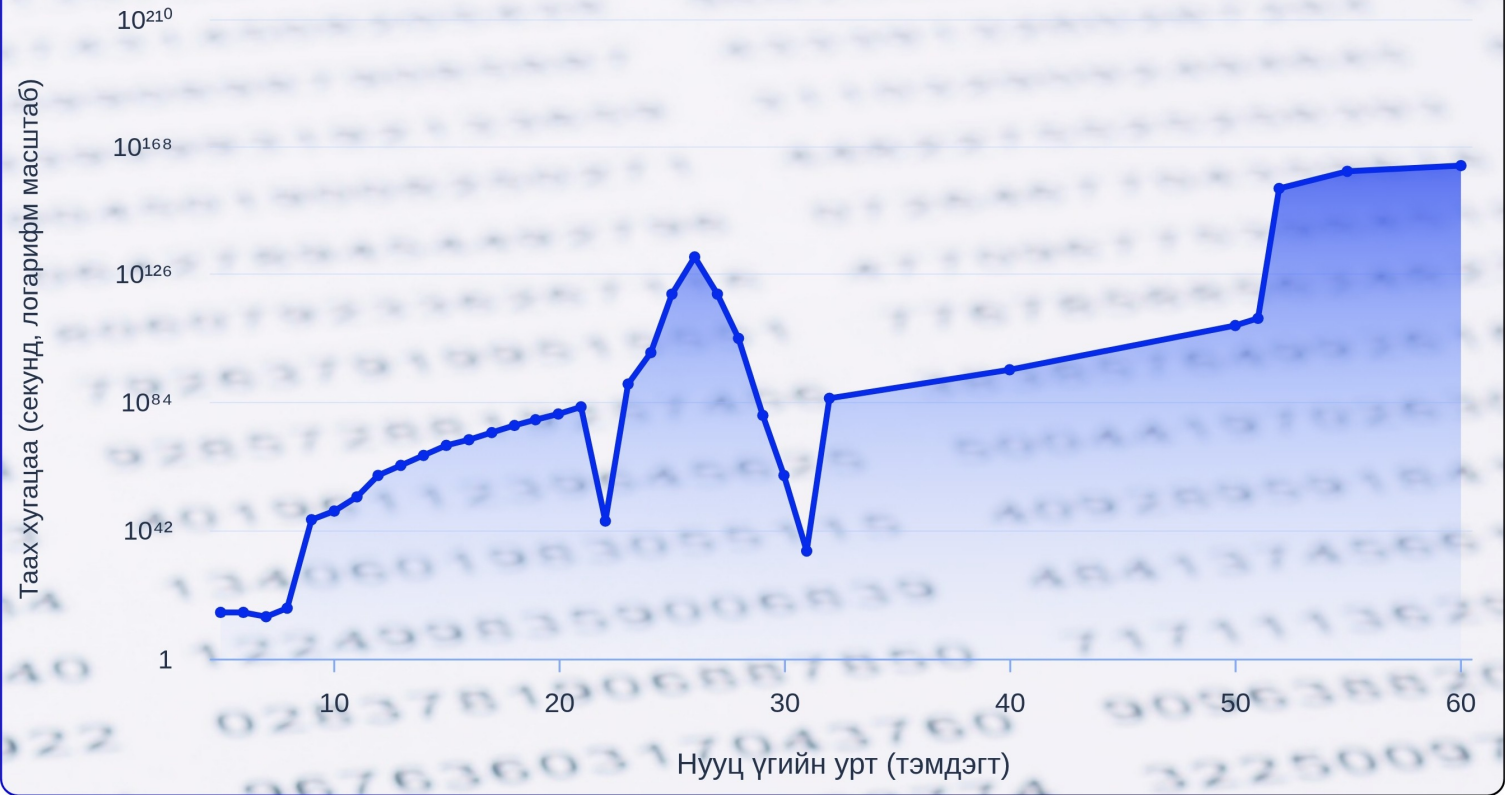
Энэхүү судалгааны үр дүн нь Монгол хэрэглэгчдийн нууц үгийн аюулгүй байдал бодит нөхцөлд хангалтгүй түвшинд байгааг харуулж байна. Мөн аюулгүй байдлын эрсдэлийг бууруулахын тулд бодлогын шийдвэр, хэрэглэгчийн боловсрол, техникийн хяналт болон стандартын хэрэгжилтийг цогцоор нь авч үзэх шаардлагатайг илэрхийлж байна.

Иймд судалгааны дүгнэлтүүд нь зөвхөн статистик шинжилгээний үр дүн төдийгүй цаашдын бодлого боловсруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлоход ашиглах бодитой суурь мэдээлэл болно гэж үзэж байна.

QR код уншуулж, дүн шинжилгээ
судалгааны тайлантай танилцана
уу.



НУУЦ ҮГИЙН УРТ БА ТААХ ХУГАЦАА



Нууц үгийн урт нэмэгдэх тусам түүнийг таахад шаардагдах хугацаа өсдөг. Гэвч зарим урт нууц үгийн таах хугацаа огцом буурч байгаа нь урт дангаараа нууц үгийн найдвартай байдлыг бүрэн тодорхойлохгүйг харуулж байна. Иймээс урт нууц үг сонгохын зэрэгцээ таахад хялбар дараалал, давталт, хувийн мэдээллээс зайлсхийж, бүртгэл бүрд өөр нууц үг ашиглах нь чухал.

ХЭРЭГЖҮҮЛЭХ 4 АЛХАМ

01

Таахад хэцүү болго

Хоорондоо холбоогүй хэд хэдэн үгээр урт нууц хэллэг үүсгэ. Нэр, төрсөн огноо, 123456 зэрэг дарааллаас зайлсхий.

02

Бүртгэл бүрд өөр нууц үг

И-мэйл, сошиал, бусад үйлчилгээ бүрд тусдаа нууц үг ашигла. Нэг нь алдагдсан ч бусад бүртгэлээ хамгаална.

03

Менежер ашигла

Нууц үгийн менежерээр урт, санамсаргүй нууц үг үүсгэж хадгал. Менежерийн үндсэн нууц үгээ мөн сайн хамгаал.

04

Давхар баталгаажуул

Олон хүчин зүйлийн баталгаажуулалт (MFA) асаа. Боломжтой бол passkey буюу нэвтрэх түлхүүр ашигла.

Нууц үг уртсах тусам таах боломжит хувилбарын тоо ерөнхийдөө нэмэгдэнэ. Харин давталт, дараалал, хэвшмэл бүтэц нь урт нууц үгийг ч таамаглахад хялбар болгодог. Урт байхаас гадна таахад хэцүү байх хэрэгтэй.



PUBLIC CSIRT/CC

КИБЕР ХАЛДЛАГА МЭДЭЭЛЭХ



113



113.mn



Pubcert.mn

GOVERNMENT PARTNER



OPERATIONAL MEMBER OF



ХАЯГ:

Баянгол дүүрэг, 17-р хороо, Амарсанаагийн гудамж,
Радио телевизийн үндэсний сүлжээ УТҮГ-ын байр,
2 давхарт, Улаанбаатар хот, Монгол улс, 15160

И-МЭЙЛ:

contact@pubcert.mn